University of Alberta

Assumed Identities: Responses to Identity Theft in an Era of Information Capitalism

by

Jennifer Robin Whitson

A thesis submitted to the Faculty of Graduate Studies and Research
in partial fulfillment of the requirements for the degree of

Master of Arts

Department of Sociology

Edmonton, Alberta
Fall 2006

Library and Archives Canada

Published Heritage Branch

395 Wellington Street
Ottawa ON K1A 0N4
Canada

Bibliothèque et Archives Canada

Direction du Patrimoine de l'édition

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file Votre référence
ISBN: 978-0-494-22182-2
Our file Notre référence
ISBN: 978-0-494-22182-2

NOTICE:
The author has granted a non-exclusive license allowing Library and Archives Canada to reproduce, publish, archive, preserve, conserve, communicate to the public by telecommunication or on the Internet, loan, distribute and sell theses worldwide, for commercial or non-commercial purposes, in microform, paper, electronic and/or any other formats.

The author retains copyright ownership and moral rights in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

AVIS:
L'auteur a accordé une licence non exclusive permettant à la Bibliothèque et Archives Canada de reproduire, publier, archiver, sauvegarder, conserver, transmettre au public par télécommunication ou par l'Internet, prêter, distribuer et vendre des thèses partout dans le monde, à des fins commerciales ou autres, sur support microforme, papier, électronique et/ou autres formats.

L'auteur conserve la propriété du droit d'auteur et des droits moraux qui protège cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

In compliance with the Canadian Privacy Act some supporting forms may have been removed from this thesis.

While these forms may be included in the document page count, their removal does not represent any loss of content from the thesis.

Conformément à la loi canadienne sur la protection de la vie privée, quelques formulaires secondaires ont été enlevés de cette thèse.

Bien que ces formulaires aient inclus dans la pagination, il n'y aura aucun contenu manquant.

Canada

Abstract

Four main themes are explored throughout this thesis. The first theme regards the construction of the identity theft threat, and how this construction furthers certain institutional interests. The second theme focuses on the relationship between information technology and what Deleuze calls a 'society of control' and how this, in turn, is encouraged by Automated SocioTechnical Environments (ASTEs) that promote an over-reliance on documentary identity and limit avenues of resistance. The third theme is one of personal responsibilization; how it is endorsed by institutions as the preeminent method in preventing identity theft, but also how it alleviates institutional accountability and furthers behaviours that benefit institutions. The final theme relates to increased surveillance and the creation of a hyper-vigilant subject who is attentive to risk. Paradoxically, this subject is so tightly bound by ASTEs and institutional processes, she is virtually powerless to ameliorate these risks.

Acknowledgement

I would like to thank both Curtis Forbes and my supervisor, Kevin Haggerty, for their support throughout this entire process.

Curtis: for the long hours commenting on my drafts, constant encouragement and willingness after two years to still argue with me about identity theft.

Kevin: for showing me how to be a teacher, academic, writer, and critic. For all the inspiration your writing and ideas have given me, and for reading countless drafts with nary a grimace.

Thank you.

I would also like to acknowledge the Social Sciences and Humanities Research Council of Canada for awarding me the Canada Graduate Masters Scholarship which has made this research possible.

Table of Contents

Chapter 1: The Conditions of Possibility for Identity Theft.....1

Chapter 2: Institutions and Identity Theft Discourses 25

Law Enforcement 26

Other Government Agencies 30

Corporate Discourses 32

Action/Inaction 37

Safety/Threat 46

Magnanimity/Self Interest 57

Competence/Incompetence 63

Chapter Three: Forging the Hyper-Vigilant Subject 74

Critiquing Responsibilization 91

Chapter 4: Identity Theft, Agency, and Resistance 99

Bibliography 109

List of Tables and Figures

Figure 1.1: Organizational Foci of Identity Theft Discourses 22

Table 1.1: Security and Crime Control Research Sites 27

Table 1.2: Other Government Research Sites 30

Table 1.3: Corporate Research Sites 32

Chapter 1: The Conditions of Possibility for Identity Theft

In early 2005 the public discovered that the company ChoicePoint had fallen prey to 'identity thieves'. A case of this magnitude—both in terms of media coverage and the number of affected consumers—propelled identity theft to centre stage. A national provider of identification and credential verification services, ChoicePoint maintains databases with billions of records about nearly every adult in America, including credit reports, criminal records, and personal profiles (CNN, 2005). This same company electronically delivered files with the names, addresses, social insurance numbers, and credit reports for almost 140,000 persons to thieves in the Los Angeles area who were posing as representatives of 'legitimate' debt collection, insurance and check-cashing businesses. The applicants were assumed to be legitimate customers because they appeared to work at registered companies in the Hollywood area. It was only upon further investigation that ChoicePoint noticed that applications for access to the ChoicePoint databases were coming from Kinko's stores and fax machines (O'Harrow, 2005).

Although the breach was found in late September of 2004, it was only publicly disclosed nearly half a year later in mid-February of 2005 (O'Harrow, 2005; Weber, 2005). In terms of victimization, at least 700 individuals have had their mailing addresses changed—apparently in order to gain control of credit card offers and other mail. More importantly, the breach and the resultant uproar over the intentional delay in alerting potential identity theft victims[1] resulted in consumer advocate calls for federal oversight of the loosely regulated data-brokering industry, and as a result Capitol Hill

[1] In fact these potential victims might not have been contacted at all if California law did not legally require companies to notify clients in the event of a security breach.

hearings were to be scheduled on the issue. The Securities and Exchange Commission and Federal Trade Commission have also launched investigations of ChoicePoint (Weber, 2005), although ChoicePoint spokesperson James Lee maintains "We're not to blame" (O'Harrow, 2005). This refusal to admit culpability is further supported by statements made by Carol A. DiBattiste, who took over as ChoicePoint's head credentialing, compliance and privacy officer in May of 2005: "I would not say mistakes were made. Mistakes to me is a culpability kind of term. I have seen very sound practices that I'm looking on improving" (Weber, 2005).

This avoidance of even partial blame for identity theft is wholly representative of institutional efforts to shirk legal and financial responsibility for identity theft and in the process avoid calls for increased institutional regulation. This is a recurrent theme of this paper, which seeks to expose how institutions, in a myriad of ways, are benefiting from the threat they have helped to create, and conversely, how individuals are subjected to multiple and diverse forms of victimization. The case of ChoicePoint and other similar events have hit institutions that deal with personal information with a tidal wave effect, and the resultant scramble to deal with this threat has thrust identity theft into the every day life of average consumers, inspiring ripples of anxiety, fear, and responsibilization.

Four main themes are explored throughout this thesis. The first theme regards the construction of the identity theft threat, and how this construction furthers certain institutional interests. The second theme focuses on the relationship between information technology and what Deleuze calls a 'society of control' and how this, in turn, is encouraged by Automated SocioTechnical Environments (ASTEs) that promote

an over-reliance on documentary identity and limit avenues of resistance. The third theme is one of personal responsibilization; how it is endorsed by institutions as the preeminent method in preventing identity theft, but also how it alleviates institutional accountability and furthers behaviours that benefit institutions. The final theme relates to increased surveillance and the creation of a hyper-vigilant subject who is attentive to risk. Paradoxically, this subject is so tightly bound by ASTEs and institutional processes, she is virtually powerless to ameliorate these risks.

This chapter sets the context for the apparent rise of identity theft and details the theory and method for how the above themes are examined. It first explores the social conditions that are conducive to the 'theft' of one's identity, focusing on technological advances which have precipitated the growth of this crime and the corresponding changes in methods of governance. One advance in particular warrants close attention: the rise of Automated Socio-Technical Environments (ASTEs) such as online shopping venues and automatic teller machines. As shown later in this chapter, such sites are key to the recent growth of identity theft.

Many of the difficulties surrounding identity and its subsequent 'theft' relate to the fact that contemporary social interaction takes place over channels created by information and communications technologies (ICTs) such as the Internet. These negate face-to-face interaction and encourage the abstraction of identity into binary flows. Social interaction can now take place simultaneously over long distances, but only by mediating the information through a technological filter (Giddens, 1990). When information passes through this technological filter (e.g. the internet, the telephone, or

even the postal system) it becomes increasingly susceptible to being split into different flows, redirected, copied, lost, and occasionally acquired by unauthorized others.

Yet it is not necessarily the case that identity theft is a new phenomenon. As stated by Canada's Office of Consumer Affairs: "Identity theft has always been a problem, but the lack of personal contact is what makes identity theft a real problem today" (Industry Canada, 2004a). Historically, citizens have placed their trust in others (e.g.. individuals, the government, etc.) because they can trace and verify the information that is provided to them. This becomes harder to do in the information age as there is an increasing reliance on technologies designed for one-way communication largely devoid of human interaction (O'Neill, 2002). As information flows become increasingly uni-directional, opportunities for dialogues which foster trust are destroyed. Even when information flows are not uni-directional, the 'conversation' and information exchange often takes place between a human and a computer whose ability to interact is limited to a list of pre-generated responses, (e.g. Thank you for your order to Amazon. Your book will be shipped in 3 – 5 business days).

Increased personal mobility combined with the technological capacity to interact with others via 'bodiless'—i.e. electronically mediated—protocols inevitably means that distant strangers interact more frequently. They share no common history and little else beyond an institutionalized relationship. They do not know each other and often know little about the institutions they are dealing with, and as such have difficulty ascertaining trustworthiness. In such a context, symbols of the stable self such as driver's licenses and credit cards rise in promise as a means to establish reputations. They act as tokens of trust in a society of strangers (Lyon, 2001: 305) and have become the access keys

necessary to enable daily interactions with others and institutions. Documents, credentials, and passwords act as indicators of reputation—easily transportable and accessible when needed—that can be assessed, created, and changed in moments—characteristics which also make them attractive to potential thieves (Nock, 1993).

Although using such tokens is often unavoidable, reliance upon such things as driver's licenses, birth dates, and credit card numbers inevitably exacerbates the issues surrounding identity theft. By providing more information on themselves, consumers are implicated in their own surveillance and in the process create further opportunities for this information to be misused. They thus "contribute to the overall movement toward greater intensification of personal surveillance, and…erode privacy because [their] autonomy in disclosing personal data is decreased" (Ball & Webster, 2003: 7). In proving their identity and consequent 'trustworthiness', individuals are paradoxically opening themselves up to the possibility of having their documentary identity stolen and losing their credibility in the process.

The conditions of possibility for identity theft are determined by the demands of information capitalism, an economic system which valorizes the accumulation of wealth and profit through the "exchange and exploitation of informational sites of value" (Wall, 2006: 593). Traditionally, economies have largely relied on the production and sale of material goods such as cars, steel, and other consumables. But in the contemporary knowledge-based economy the creation and management of information and technology drives commerce and the creation of jobs (Castells, 2000). As put so colorfully by the Canadian Office of Consumer Affair's "Privacytown", an on-line map complete with

cartoon depictions of possible privacy challenges[2] (Industry Canada, 2004a, 2004b), personal information has become a source of profit:

> **Everyone Wants a Piece of Your "Pi" ("Personal Information")**
>
> Businesses and other organizations have come to see a special value in developing an intimate understanding of existing and potential customers, to better market their products or deliver their services. This has made marketing strategies more sophisticated and aggressive, and turned your personal information into a very valuable commodity that can be bought, sold and traded by third parties. Some very elaborate sales promotions, such as customer points schemes for example, have been created primarily as a way to track the personal information of consumers and purchasing patterns, so that the information can be used or sold.

Before the advent of widespread communication networks and data storage capabilities, government, law enforcement and private companies found it prohibitively expensive to collect large reams of personal information. When collected, it often sat in paper files that were difficult to organize, manipulate, and search efficiently. The revolution in computational technologies has heralded a revolution in the gathering, storage, and manipulation of consumer data and personal information. Personal information can now be easily and cheaply assembled in massive databases to be used (and abused) in profitable new ways. The value of this information lies in its ease of collection. As expressed by Industry Canada, consumers appear largely unconcerned about divulging stray bits of information such as their postal code, birth date, or marital status, and are unaware of how this information is later compiled, analysed, and used:

---

[2] Privacytown is also home to the pseudo-scientific claim that "in a recent study, four out of five professionals recommended Privacytown as an excellent source of privacy smarts" (Industry Canada, 2004a, 2004b).

Data Mining

When you look at a single piece in a big jigsaw puzzle, you'd have to be psychic to be able to describe the complete picture. So most people don't worry when they provide a bit of personal data here and another piece of personal information there, because they're only small pieces in a very large puzzle. But when enough pieces of personal information are floating around, they can be assembled in a database to provide a fairly complete blueprint of an individual's personal likes, dislikes, habits, hobbies, buying patterns, opinions, medical conditions, financial status and lifestyle. That information can then be sifted through to pull out whatever specific information a third party wants.

(Industry Canada, 2004a)

Census bureau data and other public records are often 'mined' to create consumer information profiles. Data mining fuels a surveillant assemblage composed of many discrete surveillant systems from both state and non-state institutions. This assemblage brings together the dispersed bits of information that trail behind individuals as they carry out their daily routines. The collected data is abstracted from its territorial setting and referent, and is reassembled into a user profile, a 'data double' of pure virtuality which is used to reconstruct and predict a person's habits, preferences, and lifestyle (Haggerty & Ericson, 2000). More and more government and marketing practices are directed towards data doubles rather than their referents.

The call for access to data doubles is so great that information is increasingly gathered under false pretenses such as fraudulent research surveys and contest forms which require the surrender of personal information in order to participate (Gandy, 1993: 64). Although commonly framed as a criminal enterprise, this collection is also done by 'trustworthy' institutions. To allay customer concerns about untoward surveillance and possible invasions of privacy, certain practices are conducted under the

auspice of learning to better serve the customer. For example, according to American Express:

> To make our e-mail offers more relevant to you, we may use information you provided in your initial transaction with us, in surveys, from information we have about you as an American Express customer—such as purchasing preferences or lifestyle—and information available from external sources such as census bureau data.
>
> (2004d)

Under the auspice of catering to the consumer, the collection of information allows Amex to create minutely detailed marketing profiles on every card holder. The pretext of improving the quality of service allows Amex to target specific groups with direct marketing as well as to sell these profiles and databases to the "carefully selected vendors and business partners [American Express] works with" (American Express, 2004d). Although 'mining' and then compiling consumer information creates opportunities for this information to be misused, for institutions, the ability to 'know' and hence influence and control individuals outweighs the possible risks.

Information capitalism, built up from the information that individuals provide about themselves, is a key factor in the larger societal transformation from a disciplinary society to a society of control. The dynamics of power and control of the latter rely upon a host a routines and practices that are put at risk by the assorted dispersed activities that have come to be referred to as 'identity theft'. The technological ability for increased informational surveillance helps usher in a society of control wherein the continued flow and integrity of personal information has become paramount to the maintenance of this system.

Deleuze contrasts the society of control with the disciplinary society analysed by Foucault. Bentham's panopticon, which was popularized by Foucault, is iconic of disciplinary society. The proposed prison uses surveillance to regulate isolated prisoners who are exposed to a central guard tower. At any given moment, prisoners are unaware of whether they are being surveilled or not, thus they behave as if they are constantly monitored. According to Foucault, this surveillance works in concert with explicitly articulated behavioral norms, compelling inmates to reflect upon their own behavior and practice intense 'soul training' to align their behaviours more closely with society's norms (Foucault, 1977). In the era of disciplinary power, achieving control is dependent on the existence of discrete 'spaces of enclosure' run by the state, such as the prison, factory, hospital, and school. The individual passes from one closed environment to another—from the school, to the factory, to the hospital, etc.—each having its own unique laws and structures, independent of the others.

Deleuze, however, proposes that disciplinary control is being replaced by an 'ultrarapid', continuous form of free-floating control which is no longer dependent on spaces of enclosure. The form of control that Deleuze describes eschews discretely bounded, structured and stable spaces of control and instead embraces an amorphous control constituted by rhizomatic assemblages of both state and non-state institutions. Unlike disciplinary society, the society of control generally does not rely on direct state intervention to regulate social groups and their behaviour. Regulation is more subtle, focused simply on the prevention of undesired behavior through the use of specific techniques, practices, and knowledges explicitly designed to 'control' social interaction (Jones, 2000). The reliability of these techniques and practices is predicated upon the

ability of institutions to 'know' their subjects and to use this personal knowledge to guide subjects' actions accordingly.

The society of control is driven by the principle that "if everything can be observed, then everything can be controlled" (Ball & Webster, 2003: 14). It operates by tracing the everyday data-economy in which habits, routines, patterns, and flows are digitized, coded and diagnosed for the purposes of regulation (Elmer, 2003). Whereas in disciplinary society, surveillance generally takes the form of human observation, in a society of control, surveillance relies on technology to monitor mediated subjects and record data (Haggerty & Ericson, 2000). Information communication technologies extend the power to observe the actions of individuals and communities by closely monitoring the information produced by consumer interactions and exchanges such as credit card purchases, DirecTV/TiVo systems, and consumer loyalty cards. Observation is focused on dataflows rather than people and the digitized information streaming from consumers to businesses, government, and countless others enables governance-at-a-distance. It draws upon a host of decentralized computer databases which no longer belong to one centralized government authority to create profiles on individual citizens/consumers/clients—profiles so detailed that they are expected to predict, as well as shape, future behaviour using subtle incentives and gestures. Consumer loyalty cards present an innocuous but telling example of these developments. Shoppers who decline or merely neglect to sign up for barcoded loyalty cards can end up paying a higher price for their purchases. Even if a consumer knows their personal information is being collected, their choices are either participation, in terms of buying specifically branded products at a 'bargain', or the default punishment of a higher price (Elmer, 2003).

Another difference between a society of control and disciplinary society resides in how the body is conceptualized. In a disciplinary society people are conceived of in individualistic terms, evidenced by a reliance on files, birth certificates, and signatures. But, at the same time as power individualizes its subjects, it masses them together into a body, each individual molded by spaces of enclosures into the larger social body (Deleuze, 1992). Individuals are seen as single entities to be shaped, punished and controlled (Haggerty & Ericson, 2000). In a society of control, people are no longer perceived as unique individuals or discrete entities, they are instead approached as flows of information and a collection of quantifiable traits entered in a database. The body is envisioned as an assemblage of myriad parts and processes to be broken down for observation (Haggerty & Ericson, 2000). "Individuals have become 'dividuals', and masses have become samples, data, markets or 'banks'" (Deluze, 1997: 311). The individual is no longer the smallest possible socio-political unit, unable to be divided further, and institutions with their managerial and marketing emphasis conceive people as no more than a bundle of traits to be managed (Jones, 2000). The move to a society of control and the resultant construction and management of these "bundles of traits" is exemplified in the use of Automated Socio-Technical Environments. Used to regulate transactions and thereby the people behind these transactions, ASTEs do not act through disciplinary techniques and 'soul-training' but through faceless digital systems that determine and enforce institutionally preferred terms of access and exclusion. Control is achieved through codes and passwords that permit or reject access to information, services, and locations, and individuals are reduced to account numbers, spending habits, and marketing profiles. The disciplinary goal of normalization, of locating

'abnormal' individuals and reforming them according to the norms of society, is abandoned.

According to Michalis Lianos and Mary Douglas, ASTEs are sociotechnical environments, characterized by systems of permissions to access, which use electronic information technology to regulate our interactions with the world via devices such as magnetic gates in shopping malls and password-protected computer networks in our homes, all the way to high-tech image recognition systems in airports. ASTEs are "technology-based contexts of interaction that regulate, organize or monitor human behaviour by integrating it into a pre-arranged environment, built upon a conception of 'normality' or 'regularity' that all subjects are expected to reproduce" (Lianos & Douglas, 2000: 264). Once established, these pre-arranged environments only require human participation in the form of the input of PIN number, credit card, password, fingerprint, retina scan, etc.. Although ASTEs can involve a simple swipe of a credit card in a check out line, the largest ASTE in the context of identity theft is the internet. Instead of interacting with people to perform routine banking transactions, purchase goods, or even to report crime, individuals are increasingly interacting with and through computers and performing all of these transactions online. These environments are created not only for consumers' ease—allowing them to interact with the world from the privacy of their homes and offices—but they are also shaped by institutions to order the world in a way that is optimal for the institution: enabling rapid interchanges of information, finances, goods and services that preclude messy and costly human interaction.

What links ASTEs to the creation of criminogenic atmospheres conducive to identity theft is that security measures are wholly predicated on tokens of trust rather than interpersonal forms of verifying users' identities. In order to gain unauthorized access to information, sites, and accounts, all that is needed is an appropriated password, swipe card, or account number of someone who has legitimate access. A common example of this is credit card fraud, which the RCMP claims was responsible for losses of roughly $200 million in 2003 (Royal Canadian Mounted Police, 2004). Although a person may be denied goods and services due to lack of funds, they can gain access by appropriating someone else's legitimate credit card. When tokens of trust are reduced to de-contextualized information, this allows thieves unrestricted entrance into the system, giving them *carte blanche* to enact their crimes unrestrained by most security precautions. Security is centered not on the human user, but on the inanimate tokens they can access and deploy.

Credit card fraud commonly relies upon relatively simple techniques, as institutional security concerns often run secondary to a market-driven concern for consumer convenience. Although financial institutions monitor transactions in 'real time' looking for discrepancies in spending patterns (American Express, n.d.-e), the possible detection of fraudulent credit card use is constrained by market pressures to provide customers with convenient access to their funds. If customers judge that there are too many questions, delays, and difficulties associated with obtaining credit, businesses fear customers will take their business to other financial institutions. This prospect poses a greater danger to businesses than identity theft. For example, in the fourth quarter of 2002, fraud cost American retailers $160 million (US) while a further

$315 million was lost by mistakenly rejecting legitimate sales. Although such numbers are always suspect, they do suggest that institutional profit margins are threatened twice as much by seemingly unnecessary security precautions then they are by actual fraud (O'Hara, 2004: 109). To prevent customer dissatisfaction no identification or authorization is usually needed to access credit card funds beyond presenting the credit card (or the card number if doing business over the phone or online). As shown by a SafeCanada site, potential profits can supersede security concerns:

> Credit card and cell phone industries are quite profitable and at least some issuers would prefer to absorb the losses they might suffer from the occasional identity theft rather than forgo the income that would have been generated by those consumers. Statistics gathered by PhoneBusters in 2003 and in the first half of 2004 indicate the largest number of complaints surrounding identity theft relate to credit cards or false applications for credit cards (32 percent).
>
> (Consumer Measures Committee, 2005: 7)

It is apparent, judging from statements like those above, that issues of verification of identity often become moot as ASTEs generally gauge legitimate access by the use of legitimate entry keys, and do not differentiate between human users behind these entry keys.

Although efficient and convenient, ASTEs are a hub of risk assessment, constantly gathering and compiling personal information in order to streamline business practices. The more data that is gleaned about users of ASTEs and their behaviour patterns, the more the functioning of ASTEs can be streamlined to 'capture' and serve clientele. More importantly, the linear formulaic functioning of ASTEs reduces the complexities of human interaction into highly regulated and standardized behaviors. Lianos and Douglas emphasize the changes driven by ASTEs in the following:

> Only those parameters that the ASTE is built to evaluate are relevant and in that sense the social universe is inevitably and progressively subjected to new configurations according to new managerial priorities. *An integrated, coherent self is not necessary* for dealing with an automated system because the system has its own unshakeable coherence into which it incorporates the acts of its user on a strictly delineated domain; *the rest of the user's identity is simply meaningless* each time.
> (emphasis added, 2000: 265)

ASTEs reduce individuals into monosemic beings: i.e. card holder, social insurance number, button presser. If a computer denies access there is no prospect for argument as technology is generally conceptualized as precise, reliable, and immune to errors. Individuals tend to accept this denial of access or question their *own* practice in terms of doubting whether they input the right password or followed the correct steps (Lianos & Douglas, 2000: 264). Personal trust and the ability to negotiate become meaningless. Therefore, although convenient, ASTEs are geared to work with beings reduced to a limited range of responses. Few people can fully explain the dynamics of online encryption or what paths e-mails travel through cyberspace. Because most users are unaware of the mechanics of the technology, questioning or critique is restricted. People are merely fragmented 'activators' and in-putters. They are holders and non-holders of tokens for predetermined levels of access (Lianos & Douglas, 2000: 265), single faceted beings, numbers and data, lacking knowledge of the systems that regulate them.

ASTEs 'create' people in their technological image, standardizing human interactions through the use of highly regulated environments. To obtain service, human users must perform sequential steps at a specific speed. For example, to obtain money at an Automatic Teller Machine (ATM), users must insert the proper debit card

in the proper slot in the proper position (magnetic stripe facing down and to the right). After inputting the correct sequence of personal identification numbers, one can select the desired transaction and withdrawal amount from a pre-approved list (e.g. often in denominations of $20 bills only, and capped by a withdrawal limit of $500). The selection must be made within a time limit or the system will 'time-out' and the transaction will be denied. Furthermore, the correct sequences must be followed—especially the PIN input—otherwise there is the risk not only of the transaction being denied, but the card being confiscated and future banking privileges being withheld.

By converting users into stings of data, institutions make it easier to gather information on, classify, and 'database' consumers, ultimately transforming them from rich human subjects into bundles of quantifiable traits. The institutional reliance on ASTEs implies that social interaction, before being regulated and shaped by automated systems, is problematic for the efficient (read profitable) functioning of institutional systems. In fact, choreographed social interaction is a necessary precondition for the operation of *all* ASTEs. Daily routines such as charging a coffee at the drive-thru, checking one's email, and purchasing textbooks online etc., are all being colonized by ICTs which are predicated upon scripted, closely regulated interactions.

The increasing number of carefully regulated interactions is inextricably linked to attempts to gain risk-based knowledge. Maximization of profits and efficiency is achieved by minimizing risk. Businesses achieve this maximization by "identifying individuals, who, by virtue of their profiles, ratings, or comparative scores should probably be ignored, avoided or treated with the utmost deference and respect" (Gandy, 2003: 30). With the growth of information capitalism, ASTEs are a tool to gather this

information. By using communication technology to track members' purchases, for example, American Express has compiled "more than thirty-four million names in its international database of customers, and it has detailed knowledge of where they travel, where they eat, and, increasingly, what they buy" (Gandy, 1993: 66). In the US, 92% of websites collect personal data from their users and process them according to their commercial interests (i.e. first aggregating the data to form marketing profiles and then selling the profiles).[3] Opting out of this collection becomes a choice of exchanging data for the privilege of access to websites and services. Thus, people often unknowingly waive their rights to privacy in order to utilize services, and once this privacy has been waived, personal data becomes the lawful property of corporations (Castells, 2001). Unfortunately, this information is also readily collected by parties whose criminal activities are aided by the ease of acquiring information.

All of this has implications for criminal behaviour. A crime such as identity theft no longer requires a stolen birth certificate or forged driving license, but assorted forms of technical knowledge. Credit reporting companies in particular appear to have become a hunting ground for criminals, with the case of ChoicePoint being a well-known example. As detailed below, the amount of data that can be collected by agencies such as ChoicePoint is astounding. This information is compiled by data brokers and accessed legitimately by businesses, government, and law enforcement, and illegitimately by 'identity thieves'. The credit reports they produce include three main types of information:

> 1) Public Record information which "includes birth and death records, property records, tax lien records, voter

[3] For example, Abacus is a database of names, addresses, and information concerning the shopping patterns of 90 million households in the US. (Castells, 2001: 174)

> registrations, licensing records and court records (including criminal records, bankruptcy filings, civil case files, and judgements)"
> 2) Publicly-Available information which includes information from "telephone directories, print publications, Internet sites, and other sources accessible to the general public", and
> 3) Non-Public Information including "identifying or contact information submitted to businesses by consumers to obtain products or services (such as name, address, phone number, email address, and Social Security Number); Information about the transactions consumers conduct with businesses (such as credit card numbers, products purchased, magazine subscriptions, travel records, types of accounts, claims filed, or fraudulent transactions);
> Information from applications submitted by consumers to obtain credit, employment insurance, or other services (such as information about employment history or assets); and Information submitted by consumers for contests, website registrations, warranty registrations, and the like"
> (Federal Trade Commission, 2005e)

These profiles—containing information ranging from birthdays to bankruptcy claims to buying patterns—are sold to marketing companies, employers, landlords, insurance companies, and government agencies.

Credit reports have become prime targets of identity thieves because they represent the amalgamation of countless other databases, constituting a true 'assemblage'. They are shining examples of the acquisition capabilities of the information network. On a bureaucratic level, the categorized information in these reports seemingly becomes the sole measure of human worth. These reports are also paradigmatic examples of the temptations associated with information capitalism. The information in databases can be employed to benefit individuals, tailoring services and products to their specific needs, but it can also be used to tailor more efficient means of exploitation, or be manipulated by criminals to appropriate a person's tokens of trust.

This paper, then, is concerned with how information capitalism has provided the preconditions for identity theft's proliferation and the attendant growth of concerns about this as a social problem. Government, law enforcement, and the corporate sector rely on the continued flow of information as their lifeblood. This information can be compiled in ways that increase their knowledge of other actants (largely consumers) and allow them to 'pattern' the behaviour of actants in ways that decreases resistance and increases institutional efficiency and profits.

Instilling and maintaining trust in institutions is a vital precondition of information capitalism, as this trust is essential in maintaining flows of information. As Giddens notes, trust refers to "confidence in the reliability of a person or system, regarding a given set of outcomes or events" (Giddens, 1990: 34). Institutions walk a fine line in announcing the evils of identity theft. Although they want to frighten consumers into embracing responsibilization measures (and thus avoid the effort and expense of preventing identity theft themselves), they cannot risk creating too much mistrust of the information network. Scared consumers who are consequently unwilling to divulge their personal information put the network at risk. In such a scenario the system of information exchange is no longer a taken-for-granted 'black box'. Distrust propagates suspicious questions about who is asking for information, why they want it, and what it will be used for, all of which make it more difficult and costly for institutions to secure unimpeded data flows.

Moreover, the veracity of the knowledge required to govern individuals and lubricate the market is endangered by the fact that this information is being 'hi-jacked'. The possibility of 'contaminated' flows and unreliable data causes institutions to distrust

the informational system, and consequently places the entire economic system at risk. It thus becomes a vital institutional mandate to restore trust in the system and 'pattern' citizens into continued participation in the information network. To do so, institutions must direct flows of information away from those actants (i.e. thieves) who will use the information 'illegitimately' and thus 'contaminate' and endanger the future existence of these informational flows, and the society of control itself.

Having set the theoretical stage in this chapter, we now move to an examination of key institutional configurations around identity theft. This paper first examines key institutions that are affected by identity theft; how they are harmed, how they benefit, and how they respond. Various research sources have been drawn on for this project, but I have mainly relied on data gathered from institutional web pages devoted to identity theft. Six research sites in total were chosen. One Canadian site and one American site were selected from each of the following realms: law enforcement, private corporations, and government consumer protection agencies. These domains capture some of the main players who work through the media to define the identity theft threat. The specific research sites were selected using various criteria including the size and type of audience targeted by each respective institution, the amount of analyzable content available, and whether this content is representative of the respective field. Major links from each of these sites were also explored.

Discourse analysis is the primary method of examining the research sites. By focusing on publicly available identity theft materials, I highlight how each institution uses different constructions to position themselves as authorities, working to contour public fears as well as to support reactive policies that best serve their own interests. In

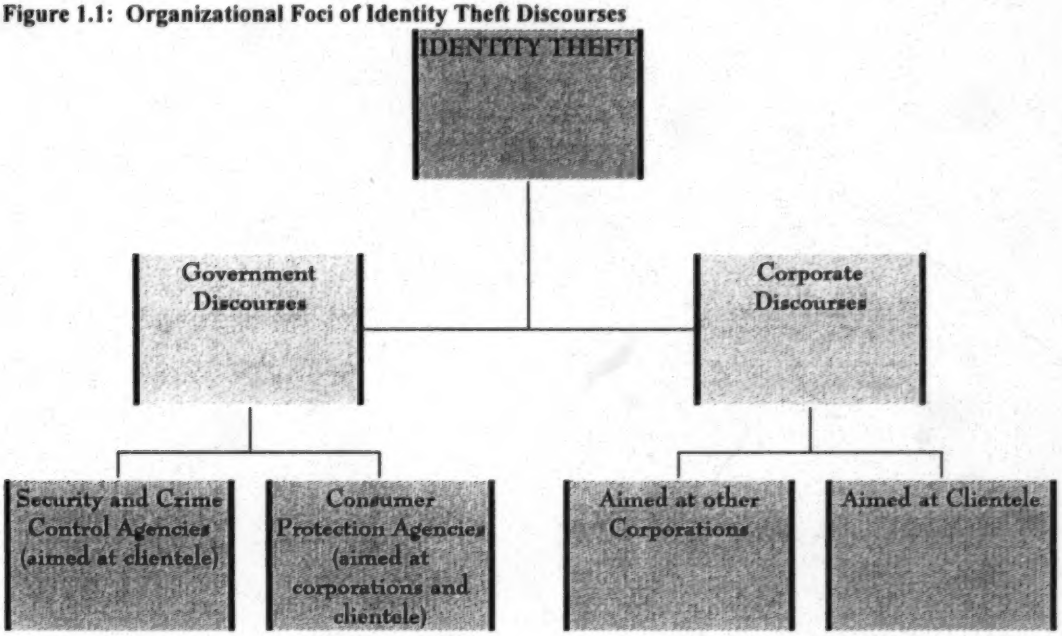
the context of this paper, discourse is defined as "the way in which language and other forms of social semiotics not merely convey social experience, but play some major part in constituting social subjects...their relations, and the field in which they exist" (Purvis & Hunt, 1993: 474). Discourses impose frameworks that limit what can be experienced and how experiences are interpreted, which then influence the actions of individuals. In terms of identity theft, institutional discourses allow certain things to be said while impeding other things, thus affecting the range of possible understandings of, and responses to identity theft.

This discourse analysis was carried out by systematically accessing and cataloging institutional on-line texts devoted to identity theft awareness and protection. These texts were then subjected to multiple close readings, with a view to highlight similar depictions of identity theft across texts as well as differences and silences. In-depth analysis is used to explore how identity theft is quantified, and how the threat it poses is shaped for public consumption. Particular focus is given to how language, in the form of suggestive words and phrases constructs a particular imagery of the identity theft phenomenon, becoming a scaffold for the performance of certain activities (responsibilization, data protection, self-surveillance) and participation in the network of information exchange.

To structure this discursive analysis, it is useful to first delineate and define the different institutions that are the focus of this analysis. In depicting identity theft, each of the above mentioned sites assumes distinct roles and scripts that are utilized to guide the public's response to identity theft. In brief, there are two main discourses, that of government and that of business. These two discourses divide into generally discrete

sub-categories as depicted in chart 1.1 below. Government discourse is divided into security and crime control discourse aimed at individuals, and consumer protection agency discourse aimed at both corporations and individual clientele. Corporate discourse is divided into that aimed at other corporations, and that aimed at individual customers.

Figure 1.1: Organizational Foci of Identity Theft Discourses


IDENTITY THEFT
Government Discourses
Corporate Discourses
Security and Crime Control Agencies (aimed at clientele)
Consumer Protection Agencies (aimed at corporations and clientele)
Aimed at other Corporations
Aimed at Clientele

The second chapter shows that although each institutional actant utilizes specific discourses and methods to construct identity theft, the final effects are similar across institutional boundaries: the reification of identity theft as a threat. Categorizing identity theft as a risk rather than a crime that can be policed and governed via traditional methods allows institutions to dissociate themselves from any and all protective obligations. Under the claim that nobody can totally prevent identity theft, they absolve themselves of responsibility for the criminogenic conditions they have helped to create. The fact that institutions benefit from the crime they purportedly abhor

creates obvious tension within and across institutional discourses. These are apparent in blatant contradictions between guarantees of safety and allegations of the harm posed by identity theft, the ostensible competence of institutions to deal with the threat versus indications and even admission of institutional inability to effectively respond to this crime, inadequate institutional actions contrasted with cries for increased action, and finally, the tension between institutional pretenses of magnanimity and their clearly self-interested motives. All of these developments cumulatively place the individual consumer on unstable ground. Over-anxious and confused, individual citizens are ill suited to recognize the threats posed by the nature and extent of identity theft and information capitalism.

Although each institution—law enforcement, government, and business—offers somewhat different definitions, descriptions, and depictions of identity theft, the role they advocate for individuals is remarkably similar. Institutional actants pressure individuals to responsibilize and protect themselves in various ways. Every institution fosters fears of identity theft in order to direct responses in ways that best serve their own agendas. Chapter three draws upon Actor Network Theory and focuses on efforts to pattern individuals' responses to identity theft in a particular direction. It is closely tied with chapter two in that the most common institutional response to identity theft has been to articulate projects for others: influencing and directing individuals' day to day behaviors in an attempt to prevent crime rather than changing the practices of institutions themselves. The information network is presented to the public as being rife with the illegitimate transfer and misuse of personal information which is pragmatically beyond institutional control. Consequently, responsibilization as a method of protection

from identity theft is advanced as the primary solution. It is simply more efficient for each individual to police themselves, their behaviour, and their data double than it is for institutions to police identity theft as a whole.

By depicting the entire knowledge network as untrustworthy except for 'authorized' nodes, institutions work to guide the flow of information from individuals, ensuring that information moves freely to institutional actants and is directed away from other, non-authorized players. Accordingly much of chapter three is focused on efforts to create a hyper-vigilant subject. Responsibilization is endlessly promoted in order to shore up weak points in the network of coordinated information transfer. The hyper-vigilant subject is fostered through 'tips' on how to avoid victimization and advice on how to respond to victimization once it has occurred. Ultimately, the panoptic gaze is focused upon the potential victim who becomes the new subject of surveillance and site of blame if a theft of personal information occurs.

In the end, knowledge about the flaws of the information system and the possible danger of this information's misuse is insufficient to prevent its exploitation. Recognizing the role institutions play in creating criminogenic conditions does not equate to the ability to change these criminogenic conditions. Citizens are patterned too well into the system of information exchange to spurn it. In exchange for the tailored and convenient services and goods it enables, it seems individuals will gladly bear the dangers. Ultimately they do so because they have no other choice. In order to flourish in a society of control, a society predicated on the exchange of knowledge, citizens must surrender their information or risk being excluded from the social system entirely.

Chapter 2: Institutions and Identity Theft Discourses

Public issues are increasingly defined in terms of their potential criminogenic qualities or adverse implications for safety and security. (Crawford, 2002: 1; Simon, 2000) Nowhere is this more clearly demonstrated than in the identity theft discourses that are at the heart of this chapter. Information transfer and the network of information capitalism is increasingly governed in terms of its criminogenic qualities and the fears that identity theft inspires. Although the content of these discourses differs, their ultimate ambitions of patterning individuals into the larger information network remain the same.

This chapter first identifies the relevant identity theft discourses and elaborates upon their composition, their origins, and how they compare to the other discourses under examination. It becomes clear that many of the complexities between and within the discourses are due to there being no single accepted definition of identity theft. One apparent constant in defining identity theft is the conception of identity theft as a risk to personal information rather than a crime against citizens. Not only do the various discourses often conflict with each other, they are often internally inconsistent. Ultimately, the purpose of this chapter is to explore these constructions and highlight how some of these tensions serve the mandate of the larger system of information exchange.

Although the methodology of this study has been covered in the previous chapter, it is beneficial to review what is meant by the term discourse and delineate which discourses constitute the focus of this study. To gather data on a range of different institutional interests, both in Canada and in the United States, research sites

were selected from the financial/business sector (American Express and the Canadian Bankers Association), the law enforcement sector (The Federal Bureau of Investigation and the Royal Canadian Mounted Police), and the government sector (The Federal Trade Commission and SafeCanada). Each of these sites and their relevance to the issue of identity theft is elaborated upon in the following sections. Security focused websites and brochures that are aimed at each of the research sites' public audiences provide the structured and regulated communication that constitutes the content of this discourse analysis. The main focus of this analysis is to investigate and explain how discursive practices (i.e. the representation of identity theft in terms of how it is symbolically depicted to the public) are bound up with forms of social organization, power, and control.

Law Enforcement

The first discourse to be examined is law enforcement. For the purpose of this project, it is constituted by two main sources; the Federal Bureau of Investigation (FBI), representing American crime control interests, and the Royal Canadian Mounted Police (RCMP), representing Canadian crime control interests. As depicted in Table 1.1, the FBI and the RCMP are connected by affiliate organizations such as the Internet Fraud Complaint Center (IFCC), Reporting Economic Crime Online (RECOL), and PhoneBusters. These affiliate organizations involve partnerships between either the FBI (in the case of the IFCC), or the RCMP (in the case of RECOL and Phonebusters) and other crime control interests. They are geared towards gathering information and statistics on crime trends, analyzing the data, and then forwarding it to the RCMP and the FBI for further dissemination.

Table 1.1: Security and Crime Control Research Sites

Organization	Acronym	Purpose	Website	Country
Federal Bureau of Investigation	FBI	Bureau in the US Department of Justice that deals with matters of national security, interstate crime, and crimes against the government.	www.fbi.gov	USA
Internet Fraud Complaint Center	IFCC	Partnership between the FBI and the National White Collar Crime Center (NW3C).	www1.ifccfbi.gov	USA
Royal Canadian Mounted Police	RCMP	Police force that operates throughout Canada except in cities and provinces with their own police forces	www.rcmp-grc.gc.ca	Canada
Reporting Economic Crime Online	RECOL	Administered by the National White Collar Crime Centre of Canada, and supported by the RCMP and other international, national, and provincial law enforcement agencies	www.recol.ca	Canada
PhoneBusters	n/a	National anti-fraud call centre operated jointly by the RCMP and the Ontario Provincial Police	www.phonebusters.com	Canada

Institutions that deal in security and crime control define identity theft far more broadly than business or other government agencies. Specifically, identity theft is depicted as enabling the commission of other, more serious, crimes and as such constitutes a threat that goes beyond stolen credit cards or fraudulently accessed bank accounts. It is a stepping stone to organized crime and terrorism, the drug trade and large scale insurance fraud. In terms of audience, law enforcement in both the United States and Canada targets individual citizens, as evidenced by such document titles as "Identity Theft: Could it Happen to You?" (PhoneBusters, n.d.-c: 1), "Don't Let this Happen to You! How to Protect Your Good Name from Identity Theft" (Federal Bureau of Investigation, 2004b), and "Protecting Yourself Against Identity Theft? Sometimes That's Not Enough" (Federal Bureau of Investigation, 2004c).

More importantly, law enforcement's own role in the crime control process has changed. Instead of taking a crime-fighting role, law enforcement agencies are

gatekeepers of information, acting as a first contact point for individuals who have either been victimized or are just looking for information on identity theft (Ericson & Haggerty, 1997; Wall, 2001). For example, although the RCMP's main identity theft webpage is less than one printed page long, this page links to Public Safety and Emergency Preparedness Canada, RECOL.ca, PhoneBusters, SafeCanada, the Government of Canada, the Canadian Consumer Information Gateway, and the FTC's Consumer Sentinel Database (Royal Canadian Mounted Police, 2003). These links provide information on reporting procedures, responsibilization tips, and exhortations to report any and all victimization, as evidenced from the PhoneBusters tagline "Fraud: Recognize It. Report It. Stop It" (PhoneBusters, n.d.-a).

The focus on statistics and the compilation of data in Canada, and to a lesser extent in the United States, serves to emphasize the information disseminating role of the police (Ericson & Haggerty, 1997). Data is compiled and analyzed in order to predict future trends, convince the public and various institutions that a threat exists, and to lobby for legal reforms and increased funding. Victim information is disseminated to other security agencies, businesses, government and finally the public, and forms their understanding of the size and nature of the identity theft threat.

These statistics are primary objects in the identity theft network. They render a simplified depiction of identity theft in the hopes of making it amenable to analysis and control. For example, by claiming that identity theft complaints to the Federal Trade Commission have increased "five-fold" from 2000 to 2002, the Department of the Solicitor General of Canada and the United States Department of Justice are justifying the claim that "identity theft has become one of the fastest growing crimes in Canada

and the United States" (Solicitor General Canada, n.d.). In so doing they heighten the anxiety surrounding identity theft and amass support for 'crime-fighting' mandates. This specific statistical claim is based on a rise of 31,117 complaints to 161,819. Although mathematically correct, this "five-fold" statistic oversimplifies the growth of identity theft and glosses over the fact that even at its 'peak', only a fraction of a percentage point of the entire American population is affected by this crime.

Furthermore, statistics are presented as objective descriptors of identity theft and are disseminated from one institution to another to become the basis upon which many institutional decisions are carried out (e.g. the FTC repeats statistics from the FBI which are then repeated by American Express). The primacy of statistics in institutional decision-making processes is closely related to the drive for governance-at-a-distance. As stated by Haggerty,

> Contemporary governmental practice relies on statistical knowledge of the objects to be governed. Distant places, people, and things are mobilized through inscriptions. These are returned to a centralized locale where knowledge accumulates and is aggregated into indicators. Reduced to simple indices, the knowledge then circulates to other state and non-state agencies. Thereby, complex and previously invisible processes become objectified and singled out as the target of governance.
>
> (2001: 88)

While central to processes of governance, the statistics on identity theft structure knowledge into predetermined formats and categories, oversimplifying the complexities of identity theft in order to make it amenable to institutional renderings of what it is supposed to be and how it should be responded to. These statistics are central to a public politics of claimsmaking and form the basis for nearly every—if not all—declaration about the rising threat of identity theft (Best, 2001).

Other Government Agencies

Government discourse about identity theft is largely geared at consumer protection measures. In the United States, the Federal Trade Commission (FTC) acts as the main consumer protection agency in terms of identity theft, as it is directly concerned with the prevention of fraud, deception, and unfair business practices. In Canada, one website, SafeCanada.ca, performs similarly to the FTC, but instead of representing just one organization it comprises numerous links to other federal and provincial government departments that address public and consumer safety issues.

Table 1.2: Other Government Research Sites

Organization	Acronym	Purpose	Website	Country
Federal Trade Commission	FTC	Enforces federal consumer protection laws that prevent fraud, deception and unfair business practices, such as identity theft	www.consumer.gov/idtheft	USA
SafeCanada	n/a	Provides public safety information from all relevant federal and provincial government departments, including Public Safety and Emergency Preparedness Canada, Department of Justice, and Department of Foreign Affairs	www.safecanada.ca	Canada

Government discourse is the most prolific in content, and is permeated with public awareness information and risk management techniques. For these agencies "identity theft refers to all types of crime in which someone wrongfully obtains and uses another person's identifying information for the purpose of fraud or other criminal activity, typically for economic gain" (Bi-national Working Group on Cross-Border Mass Marketing Fraud, 2004: 2). Although this definition is broader than corporate definitions, the focus on identity theft and fraud rather than the entire spectrum crimes that are enabled by stolen identities makes it less expansive than those of law

enforcement. Attention is directed towards consumer protection by elaborating how individuals' personal information can be accessed and misused, but this information is also supplemented with a small amount of material explicitly aimed at small businesses, such as "Identity Theft: Protect your Business, Protect your Customers" (Federal-Provincial-Territorial Consumer Measures Committee, 2005), and "Information Compromise and the Risk of Identity Theft: Guidance for Your Business" (Federal Trade Commission, 2004a). These documents contain similar information as that provided to individual consumers, but include supplements to help companies "investigate the problem internally, and devise a plan for notifying people outside of the organization". Examples of these supplements include notification letters that can be personalized using 'cut and paste' techniques (Federal Trade Commission, 2004a) as well as tips on how to "avoid liability in a civil action" (Federal-Provincial-Territorial Consumer Measures Committee, 2005: 12), suggesting that businesses identify a different set of risks under the rubric of 'identity theft'—a topic that will be discussed later in this chapter.

The tone of the governmental identity theft discourse is distinct from either law enforcement or business, as government agencies take a practical and detailed step-by-step approach with the public (despite still being somewhat alarmist). Of the three, this discourse is the most concerned with providing individuals with clear information on their legal rights, exact steps to take if victimized[4], and contact information for whom they should notify. In fact these agencies are the only sites that distribute information

[4] Both SafeCanada and the FTC advocate following four main steps once victimized: 1) View and place a fraud alert on one's credit report, checking the report periodically throughout the next year and looking for irregular information. 2) Notify financial institutions and close any accounts that have been tampered

on legal rights and remedies for victimization, including sample letters on how to dispute fraudulent bank account information, as well as details about blocking fraudulent information on one's credit report and responding to criminal charges, (Federal Trade Commission, 2005g). As such, they are primary actors in patterning individuals' responses to identity theft. Business discourses, in comparison, are largely silent on what to do after victimization occurs, favoring instead to maintain the impression that victimization only happens to *other* people doing business with *other* competitors, whereas law enforcement sources provide little beyond statistics, apparently preferring to rely on other government agencies to provide the rest.

Corporate Discourses

The corporate discourses in this study were specifically chosen for their links to the financial industry, which is portrayed as having the most to lose due to identity thieves. American Express, based in the United States, was selected because of its worldwide reach and portfolio that includes investment products, insurance, and credit card services, and also because it is recognized as being forefront in the field of collecting, storing, and utilizing the personal information and spending profiles of its clientele. The Canadian Bankers Association was chosen to provide a Canadian corporate research site, and also because of its influence with the Canadian banking industry, the police, and the government in developing public policy pertaining to the financial industry.

Table 1.3: Corporate Research Sites

Organization	Acronym	Purpose	Website	Country
American Express	Amex	Worldwide financial services company based in the United States which operates in	www.americanexpress.com	USA

with or opened fraudulently. 3) File a report with one's local police. 4) File a complaint with the FTC or the Canadian equivalents; PhoneBusters, or RECOL.

		more than 130 countries. It is a leader in charge and credit cards, Travelers Cheques, travel, investment products, insurance and international and online banking.		
Canadian Bankers Association	CBA	Professional association that provides chartered banks of Canada with information, research and operational support and contributes to the development of public policy on financial services. The CBA also provides information, statistics and publications to help individuals and small businesses manage their financial affairs.	www.cba.ca	Canada

American Express, echoing corporate identity theft discourse more generally, defines identity theft "as a type of fraud in which someone uses your name and personal information to open new accounts, and then makes fraudulent purchases" (American Express, n.d.-f). In comparison to the other discourses, this is a narrow categorization related only to the financial motive of identity thieves; to obtain money and consumable goods. This is indicative of the fact that businesses are not interested in the criminal event itself. What matters to them is avoiding the damages associated with the theft, both financially and, perhaps more importantly, in terms of their reputation as a secure business.

From this brief outline, it is apparent that all institutions have somewhat distinctive conceptions of identity theft. Accordingly, there is difficulty in objectively measuring and responding to the risk of identity theft. It also makes it difficult for individuals to arm themselves with institutional knowledges about what identity theft is and how to protect oneself. Yet, across all institutions, identity theft is a 'catch-all' term

for multiple forms of *fraud*, as evidenced by the FTC's report on National and State Trends in Fraud and Identity Theft:

> Credit card fraud (28%) was the most common form of reported identity theft followed by phone or utilities fraud (19%), bank fraud (18%), and employment fraud (13%). Other significant categories of identity theft reported by victims were government documents/benefits fraud and loan fraud.
>
> (Federal Trade Commission, 2005d: 3)

And although institutions disagree on what specific crimes qualify as identity theft, the association of the crime with risks to the system of informational exchange is a commonality.

Much of the complexity surrounding identity theft discourses arises from labeling identity theft as a technological risk rather than a crime that can be policed and regulated via traditional methods. Identity theft is depicted as being closely tied with technological innovations such as the internet, and consequently cybercrime is commonly conflated with identity theft or portrayed as a subcategory of it. This technological aspect presents challenges for its regulation, as shown later in this chapter.

It is because thieves purportedly have numerous methods of gleaning information, from dumpster diving to hacking, that identity theft's complete elimination is often presented as being nearly impossible. For example, it is commonly pointed out that:

> Simply by doing things that are part of everyday routine – charging dinner at a restaurant, using payment cards to purchase gasoline or rent a car, or submitting personal information to employers and various levels of government – consumers may be leaving or exposing their personal data where identity thieves can access it and use it without the consumers' knowledge or permission.
>
> (Solicitor General Canada, n.d.: 2)

Identity theft thus seems like an inescapable eventuality tied to routines of daily life. Acknowledging that identity theft is "growing because more personal information is collected and retained than ever before, and the risks of theft multiply every time that information is transmitted or retained or disposed of in an unsafe manner" (Federal-Provincial-Territorial Consumer Measures Committee, 2005: 2), casts the problem in terms of the governance of information transfer. Identity theft is not attributed to systemic flaws in the information gathering process nor information capitalism in general, the blame is focused on individuals (both criminal *and* non-criminal) and assorted 'flaws' in their behaviour. The system of information capitalism is not to blame, but rather individuals who do not behave responsibly within the system are.

By embedding the risk of identity theft into everyday life, institutions 'off-load' responsibility for this crime onto individual citizens. It becomes a hazard to be avoided and is normalized alongside other 'risks' that individuals must manage on a daily basis, akin to putting on sunblock to avoid the risk of UV damage or steering clear of cigarette smokers to avoid the risk of cancer. As such, it is characteristic of many crimes in the 'risk society', where the moral element of crime is commonly lost or re-moralized (Beck, 1992; Garland, 2001). Instead of addressing offenders, institutional practices, or even the social system that perpetuates offending, responsibility for risk avoidance is placed on the potential victim.

For individuals, estimating the risk of identity theft is a difficult and uncertain business because the mechanics of information transfer are commonly unknown, both online *and* in the physical realm. The public are largely unaware of the workings of online interaction such as how websites collect information, where information is stored

once it is collected, and who can access it. Such ignorance is not restricted to technological methods of information transfer, but also extends to face-to-face occurrences. People seem just as uninformed about the dynamics of person-to-person information transfer, (e.g. when talking to their banker, employer, or insurance adjuster). What this information will be used for, how it will be stored and for how long, and how many people have access to it all remain unknown.[5] Thus many decisions about potentially risky activities are made by citizens on the basis of informal perceptions of how information should be handled and how risk should best be mitigated. These informal perceptions are often formed via exposure to institutional sources, such as the official websites of credit card companies or banks, which commonly have complicated motives. Government agencies and law enforcement also benefit from emphasizing the risk of identity theft and promoting responsibilization measures, as they shift the financial burden for protection efforts onto the individual (as well as the blame when something goes wrong).

Each discourse introduced above assumes different roles and scripts in their response to identity theft. Yet they share similar goals and techniques. Regardless of whether the focus is on providing statistics identity theft, or providing tips for avoiding victimization, or even re-establishing trust relationships between consumers whose faith (and spending patterns) may have been altered, the result is the same: Reifying the identity theft threat, and bringing it into the home of every consumer. By using the term "reify", I mean to express that although there are real dangers posed to personal information, institutional conceptions of identity theft lump together disparate crimes (e.g. using a stolen credit card, terrorist activities, mortgage fraud, etc.) into one

[5] Or at least buried within pages of fine print and legal jargon.

category, whose linkages, similarities, and relationships with each other—beyond the title of identity theft under which they are all subsumed—are highly questionable.

The incongruencies *between* and *within* institutional discourses place citizens upon unstable epistemological ground. These contradictions can be centered along four main axes: 1) safety/threat, 2) action/inaction, 3) magnanimity/self-interest, and 4) competence/incompetence. Detailing the tensions within these four axes will reveal how conflicting knowledge claims, institutional directives, and ambiguous advice create the conditions for a confused and anxiety-riddled citizen, one who is unsure of where they stand or of their responsibilities, and thus is amenable to being further molded to fit within the information network.

Action/Inaction

The first tension in these discourses concerns the frequent cries for 'something' to be done about identity theft, which contrast markedly with the silence surrounding what the institutions who are voicing these cries are doing themselves. Arguably, publicizing identity theft and focusing public awareness on the issue could be construed as activity, but instructing other parties on how to address crime is comparatively passive, and not directed at 'fighting' crime itself. It seems that it is easier to broadcast calls for action than it is to break institutional inertia and take action in response to identity theft. Institutions, when they do respond to identity theft, are not agents of change. Their responses lack immediacy and instead concentrate on drawing consumers into responding to identity theft. Focusing on certain responses (e.g. printing educational material) often disguises the fact that more important responses (e.g.

attempting to arrest and prosecute perpetrators) are being ignored. Demands for legislative reform are the first 'call for action' to be examined in this section.

By legal definition, fraud is interchangeable with identity theft and is addressed in Canadian and American criminal codes along with forgery, theft, trafficking in credit and debit card data, interference with computer data, and impersonation offences. But identity theft itself is a relatively new addition to legislation in the United States and is not yet added to the Canadian Criminal Code. In the United States, *The Identity Theft and Assumption Deterrence Act* was enacted by Congress in 1998, making identity theft a federal crime. Under federal criminal law identity theft occurs when someone "knowingly transfers, possesses or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law" (Federal Trade Commission, 2005g: 35).

In Canada, there are multiple arguments for new legislation, the first being that existing gaps in criminal law facilitate identity theft. For example, the Canadian Bankers Association argues that "the mere possession of multiple pieces of identification for a number of individuals, the possession of 'personal information' of another person; and the manufacturing or possession of 'novelty' identification," should all be constituted as crimes based on possible linkages to the rise of identity theft (Canadian Bankers Association, 2003b: 2). This considerably expands the jurisdiction of both law enforcement and government, resulting in a form of function creep. Behaviours not ostensibly related to identity theft, such as using an older sibling's

identification to sneak into the local bar, or carrying birth certificates for one's children could be conceived of as offenses, thereby increasing the realm of actions to be governed and policed. The CBA further argues that a) the existing criminal code contains many outdated and overlapping areas, and b) that current technologies are instrumental in the commission of identity theft, and the Criminal Code needs to be updated to keep pace with these technologies.

Government agencies differ from most businesses in terms of their support for legal reforms and increased involvement of law enforcement. These agencies advocate openness when institutions face a security breach, endorsing the participation of law enforcement and prompt notification of all clientele involved (Federal-Provincial-Territorial Consumer Measures Committee, 2005). Unlike corporations, government agencies (along with the Canadian Bankers Association) see legislative reforms as appropriate and successful responses to identity theft, as indicated by frequent references to anti-identity theft legislation and/or the lack thereof in Canada, as well as a lack of emphasis on technology upgrades and computer security measures (Canadian Bankers Association, 2003b; Federal Trade Commission, 2005g). The Canadian Bankers Association straddles the domain of both government and business. Although the CBA depends on consumer trust and business, it is also rooted in strict regulatory practices and procedures more akin to government than the corporate world. This dual personality is seen in its response to identity theft. Whereas the business element of the CBA emphasizes increased security expenditures in response to identity theft, such as the $4 billion spent on security and technology upgrades in 2002 (Canadian Bankers Association, 2003a), the government element strongly pushes for legal reforms.

Corporate identity theft discourse differs from government and law enforcement in that it does not focus on perpetrators. Even though corporations often discuss identity theft *methods* such as "mail stolen from a mailbox; Change of address forms redirecting the destination of your mail; Home computers infected with viruses that transmit data to thieves…", *perpetrators* do not seem to exist beyond explaining how identity theft happens and how individuals can protect themselves (American Express, n.d.-g: 1). Although government and law enforcement themselves are only marginally concerned with perpetrators, the complete corporate indifference to perpetrators can be explained by examining the rationale underlying institutional responses. Law enforcement and government agencies rely on legislation for increased power and jurisdiction. In the case of identity theft, this legislation is often criminal law dependent on a victim/offender dichotomy. If there is no offender, there can be no crime. Conversely, corporations commonly do not depend on legislation for problem solving. Catching perpetrators and 'bringing them to justice' is inefficient compared to quietly shoring up security breaches, because publicity about identity theft causes more reputational damage than harms suffered from the crime itself.

For security concerns that cannot be adequately dealt with in-house, businesses often turn to private firms that offer forensic accounting and corporate investigation services (Williams, 2005). Staffed by accountants, lawyers, investigators, former police officers, and computer analysts, these firms offer a broad spectrum of services, from legal advice, to technological upgrades, to tracking errant information flows, thus avoiding the necessity of involving multiple organizations to meet each separate need. Importantly, these firms offer discrete solutions that do not involve outside sources such

as media or the police, which are essential in maintaining the trust (and business) of clients and investors wary of companies that are under official police investigation.

The rise of forensic investigation services allows corporations to define who and what is open to investigation, and thus exert control over how incidents are problematized and disseminated to the public, if they are disseminated at all (Williams, 2005). Investigators ignore questionable activities that may have financial or reputational consequences for their corporate clients, thereby avoiding public recriminations about practices that enable security breaches or information leaks. These firms can investigate occurrences that fall beyond the criminal code, thus allowing them to avoid some of the difficulties faced by law enforcement when attempting to regulate the internet.

Forensic accounting services are only one method that corporations use to govern information and problematize identity theft in their own terms. Hierarchies of notification are another area in which corporations respond differently than government agencies, which are relatively eager to notify law enforcement, customers and outside organizations in order to reduce potential damage and "avoid liability in a civil action" (Federal-Provincial-Territorial Consumer Measures Committee, 2005: 12). In the case of corporations, the notification process is quite complex, and coercive and punitive arrangements often underlie reporting requirements. For example, merchants doing business with American Express must notify Amex "immediately after learning of a possible compromise" or risk being held liable for fraudulent transactions (American Express, 2004b). Responsibility for notifying others ends there. If merchants suspect that information has been compromised, their sole duty is to contact their Amex Client

Relations Manager or Telephone Service Center and await further instructions. There is no directive to contact the police. Merchants are reassured that "American Express is [their] partner in resolving these issues and will respect [their] request for confidentiality," and that information will never be released to the press (American Express, 2004c). This leads to two assumptions: 1) that any security compromises are a private matter to be settled by Amex and its merchants, and 2) there is an unequal relationship between Amex and its merchants, wherein Amex holds the power to decide how to address the security breach and whether or not to notify the police and potential victims.

In addition to their reliance on legal solutions as adequate responses to identity theft, government agencies also work to influence other institution's responses to identity theft through the provision of "outreach and informational materials to businesses about best practices" and "law enforcement training and consumer education materials to federal, state and local law enforcement and other agencies" (Federal Trade Commission, n.d.-a). According to the FTC, they have "taken the lead in producing and promoting educational material to increase consumer awareness and to provide tips for minimizing identity theft" and have instituted identity theft training seminars for over 2,200 law enforcement officers (Federal Trade Commission, 2005b). Comparable practices are also followed by the CBA and SafeCanada (Canadian Bankers Association, 2003b; SafeCanada, 2005). In this way, government agencies disseminate their specific construction of identity theft, and endorse how they believe consumers, businesses, law enforcement and even other government agencies should respond to this crime. For example, the FTC hosts a toll-free telephone hotline, an online complaint

form, and an information site all dedicated to identity theft issues which receive approximately 15,000 to 20,000 contacts per week. In addition, the "FTC alone has distributed more than 1.4 million copies of the *Take Charge* booklet since its release in February 2000 and has recorded more than 1.8 million visits to the Web version" (Federal Trade Commission, 2005f). Each contact, be it via telephone, internet, or in paper form, is an opportunity for the FTC to broadcast their views on the extent of the identity theft threat:

> Overall, nearly 10 million people – or 4.6 percent of the adult population – discovered that they were victims of some form of identity theft. These numbers translate to nearly $48 billion in losses to businesses, nearly $5 billion in losses to individual victims, and almost 300 million hours spent by victims trying to resolve their problems. Moreover, identity theft is a growing crime.
>
> (Federal Trade Commission, 2004b)

Other institutions with differing calculations of the extent of identity theft have less opportunity than the FTC to broadcast these calculations. The materials distributed by the FTC transmit its specific views on the extent of identity theft, and further relays its beliefs on how the public should react to this crime.

Paradoxically, law enforcement—who by definition seem the most accountable for responding to crimes such as identity theft—are largely silent on what specific actions they are taking to counter identity theft, except for listing the creation of new task forces and programs:

> The FBI has undertaken the following initiatives to combat cyberterrorism: Cyber Task Forces, Public/Private alliances, International Cyber Investigative Support, Mobile Cyber Assistance Teams, Cyber Action Teams, Cyber Investigators Training, a Cyber Intelligence Center, and Cyber Tactical Analytical Case Support.
>
> (Lourdeau, 2004)

Yet these programs, their structure, their purpose, and details on their functioning are never elaborated beyond their impressive titles. The only other response specific to law enforcement is the support of cross-jurisdictional cooperation between police forces:

> The protection of our networked systems is a shared responsibility and partnership between the private sector, state and local law enforcement agencies, U.S. Federal Law Enforcement agencies, the Department of Homeland Security, and the Intelligence Community, both domestic and foreign. The FBI encourages international cooperation to help manage this increasingly global problem.
>
> (Lourdeau, 2004)

Police discourse implies that information communications technologies (ICTs) have generated the conditions for the emergence of crimes which fall outside of the current criminal justice paradigm. Thus new levels of understanding and techniques of policing are required. The criminal potential of the internet, coupled with the undesirability of policing it has caused law enforcement to change its technique, as shown by the following quote:

> Remember: There is no reason to be paranoid; there's just reason to be careful. If someone wants to target you, they can probably get a lot of information about you – so you just need to minimize the criminal's opportunities to get that information. You can make yourself a harder target and that [*sic*] the best defense.
>
> (PhoneBusters, n.d.-c)

In relation to the internet, law enforcement no longer claims to defend citizens. The only person who can prevent an identity from being appropriated for criminal endeavors is the individual herself, and not the police. Thus when victimization occurs it is not seen as due to lapses in policing, but rather because individuals did not defend themselves properly.

The silence about what preventative actions institutions are undertaking is most apparent in law enforcement, but is by no means restricted to this realm. Although less noticeable, government agencies and private corporations are also reticent in detailing their responses identity theft. As alluded to by the above examples, institutions fill the silences with talk on current and upcoming legislation and protective methods they believe citizens should adopt, and thereby gloss over details of their own responses to identity theft, masking institutional inactivity when it comes to reforming their own risk-producing practices. All institutional sites have helped create the identity theft threat via practices that privilege personal information and make it a target of thieves, and alternatively, by inflating the amount of danger inherent in identity theft. Yet institutions avoid responsibility and blame. By focusing on horror stories, statistics, and avoidance tips, institutions shift the discussion away from conditions that enable identity theft and instead promote the idea that except for victims themselves, no one seems accountable for identity theft—not insecure institutions with criminogenic business practices and not even perpetrators themselves. In general, the 'actions' institutions take against identity theft are those that problematize the crime according to their own terms.

As demonstrated in the subsequent section and in the following chapter, institutions walk a fine line in announcing the evils of identity theft. Chapter one introduced the idea that although institutions want to frighten consumers into responsibilization measures, they cannot risk creating too much mistrust of the information network. This issue of trust introduces us to the next axis: Safety versus Threat.

Safety/Threat

According to Onora O'Neill, if "the developed world is the paradigm of a 'risk society', risk societies must be characterised simply by their *perceptions of* and *attitudes to* risk, and not by the seriousness of the hazards to which people are exposed, or the likelihood that those hazards will harm them" (O'Neill, 2002: 16). As a crime which has purportedly affected over 10 million Americans in the 12 months preceding a 2003 survey (Federal Trade Commission, 2004b), there is a discursive theme that presents everyone as at risk of identity theft. But it is necessary to contextualize the harm caused by identity theft. If it is a case of debit or credit card fraud, then personal financial harm is minimal or non-existent—legally limited to a $50 deductible in the United States, and fully reimbursed by Canadian banks and most credit card companies (American Express, n.d.-d; Canadian Bankers Association, 2003a; Federal Trade Commission, 2005g: 13). Even harm caused to financial institutions seems to be negligible: "[w]hile Visa Canada and MasterCard Canada incurred losses of $134.10 million in 1999, and $163.18 million in 2004, these losses represent only a small percentage of the banks' overall sales volume (less than 1 percent)" (Consumer Measures Committee, 2005: 7). Financial institutions generally seem willing to accept at least some, if not all, of these losses as negligible costs of doing business.

The tension between stressing the harm of identity theft and then asserting that individuals are safe from identity theft is effectively illustrated by American Express. Amex vocalizes two different discourses: one aimed at individual clients and one aimed at businesses. They similarly stray away from discussing how corporations contribute to identity theft through business practices such as the electronic collection and storage

of personal information, and targeted mail-outs promoting easy credit opportunities, both of which—along with numerous other practices—can be intercepted and misused by potential identity thieves. Despite these similarities, corporate and clientele discourses provide conflicting information, and apparent inconsistencies exist even within these discourses as a result of Amex simultaneously attempting to establish identity theft as a possible threat while assuring clientele and business partners of their security and safety.

Consumer discourse wavers between warning consumers about the general threat of identity theft and reassuring consumers of their safety. For example, although American Express acknowledges that identity theft can occur and "is the top consumer fraud complaint"[6] (American Express, n.d.-g), Amex also avows through its Fraud Protection Guarantee that cardholders will not be held responsible for fraudulent charges: "Use the American Express Card and you won't be held responsible for any fraudulent charges. Period. No fine print, no deductible-just pure protection so you can shop with confidence anywhere online or off"(American Express, n.d.-b). Yet, this does not prevent Amex from offering profitable identity theft insurance and other security measures, an issue discussed in detail later on. Corporations are eager to discuss general identity theft trends and statistics, referring to identity theft as "the fastest growing crime in North America" (Canadian Bankers Association, 2003b), and they are also eager to promote purchasable security options, such as Identity Protection Insurance and credit report monitoring systems. Yet they are silent about losses faced by individual

[6] This claim is not surprising given that almost all fraud can be subsumed under the category of identity theft.

corporations, especially those faced by the corporations, such as American Express, that are marketing these security options.

Corporations emphasize "accurate, confidential, and secure" information practices (Canadian Bankers Association, 2004a), and the provision of detailed privacy statements accounting how information is collected, used, and stored (American Express, 2004d, 2005c) to encourage customers to trust that their information and capital is dealt with in the most discreet and secure manner. In fact, tension about issues of trust is evident in all institutional identity theft discourses. There is constant negotiation between trusting institutions to protect information when faced with the seemingly unstoppable threat of identity theft. In the event of victimization—which is often portrayed as unpreventable even with the most secure technology—customers are reassured that the company will absorb any financial losses within days: "in the unlikely event that a fraud does occur, our customers will get their money back, usually within 5 to 7 business days" (Canadian Bankers Association, 2003a).

The most apparent difference between corporate discourse aimed at clientele and discourse aimed at other businesses is how the damage of identity theft is portrayed and ultimately addressed. For businesses, losses have more to do with security costs and upgrading technology than the actual financial loses caused by identity thieves. The cost differential between the price of upgrades and the actual damage caused by identity theft can be staggering. For example, in 2002 security and technology upgrades for Canada's banking industry amounted to over $4 billion (Canadian Bankers Association, 2003a), whereas it is estimated that identity theft costs the *entire* Canadian economy only $2.5 billion per year (Canadian Bankers Association, 2003b). From these statistics

it can be inferred that businesses stand to lose more from customers taking their business and money elsewhere than from the actual theft. Consequently, businesses expend vast amounts of money convincing customers that their information and money is safe in corporate hands.

The tension caused by the dichotomy between safety and threat is also apparent within law enforcement discourse. Although American and Canadian police both consider identity theft a problem, their conceptions of its extent differ by a substantial degree. To appreciate and account for this divergence, it is necessary to provide some background. The type of information presented by each country's law enforcement agencies and the tone in which it is presented exemplifies the differences between American and Canadian law enforcement discourses. In Canada, disseminated material is largely based on gathering statistical information and pinpointing trends. For example, both RECOL and PhoneBusters, and the FBI's Internet Fraud Complaint Center (IFCC) in the States, are primarily geared at statistical analysis of identity theft occurrences and reporting these findings to the appropriate law enforcement agencies. But the charts and statistics created by the IFCC are less visible to the public, merely used to punctuate another conversation. Dramatic accounts and cautionary tales replace the impersonal numbers and calculations found in Canadian law enforcement sources. An example of this can be found in the posting, "A Conundrum: How Do You Prevent Crimes That Haven't Been Born Yet":

> The Problem? The fact is, the interconnectedness of the Internet with national infrastructure systems has created a whole new landscape to commit crimes, and a whole new set of tools to commit them – a fact that terrorists and criminals are just beginning to understand.

> That's why the FBI – with its state, local, federal, international, and private sector partners – is working to get out in front of plots and schemes that are still in their formation stages. Awful things, too – such as using Internet tools to launch cyber attacks on infrastructure systems in tandem with physical attacks…potentially paralyzing a city, a region, even the nation.
>
> (Federal Bureau of Investigation, 2004a)

There is an emphasis on technological threats, especially in relation to how a networked American society allows outsiders, including terrorists and other criminals, access to national defense networks. In the interest of national security, the threat of identity theft zenophobically expands to encompass national security threats such as foreign terrorists who assume American identities to evade the FBI.

Despite similar difficulties in policing identity theft, American and Canadian law enforcement diverge greatly when looking closely at specific research sites. For the FBI and American law enforcement in general, the identity theft risk is closely linked with the rise of technology and cyberterrorism. Identity theft purportedly allows foreign terrorists to masquerade as insiders who "have unfiltered access to sensitive computer systems" (Lourdeau, 2004). The FBI thus paints a picture of terrorists, using techniques that can be subsumed under the category of identity theft, electronically attempting to gain access to large-scale distribution systems, "such as those involving natural gas, oil, electric power, and water, [which] tend to use automated supervisory and data acquisition (SCADA) systems for administration." These SCADA systems are presented as having multiple vulnerabilities that make them particularly susceptible to attack, including poor computer security, lack of encryption, and poor enforcement of user privileges (Lourdeau, 2004). Once access is gained to networked systems, there is the potential for a large scale attack with national repercussions.

Canadian perceptions of perpetrators and the nature of risk are much different. The risk of identity theft is more diffuse and any mention of individual perpetrators or a link between terrorism and identity theft is completely absent from RCMP, RECOL, and PhoneBusters sites. Instead of cyberterrorists using stolen identities to access and sabotage the national infrastructure, Canadian descriptions of identity theft are less threatening and more prosaic. Thieves are depicted as using stolen identities to "apply for loans, credit cards and other services, purchase vehicles, take luxury vacations, and so on" (Reporting Economic Crime Online, n.d.).

As shown by the above examples, the dichotomy between safety and threat is prevalent in identity theft literature, both in terms of law enforcement and business, but also in terms of institutions as a whole. There are multiple reasons detailing why institutional approximations of the identity theft threat fluctuate so wildly. Perhaps most obviously the differences between American and Canadian discourses can be explained by dissimilar political climates. After the terrorist attacks of 9/11, the United States is a nation perpetually on guard, suspicious of outsiders, and wary of attack. It is a nation at war. It takes little to convince the public that they are at risk, and links are made between identity theft, computer crime, and possible strikes at national infrastructure. Dramatic anecdotes of identity theft are presented at face value, not needing the support of facts and figures.

Although cyberterrorist attacks have been "limited to relatively unsophisticated efforts such as the email bombing of ideological foes or the publication of threatening content" (Lourdeau, 2004), cyberterrorism has become increasingly important in national and international crime control circles. In the United States, everything,

including identity theft, is now read through the lens of terrorism. Perhaps this is because "trust and confidence in the systems that support commerce, communications, air traffic control, electric power generation and other modern institutions are at the very core of our society. Thus, even the potential for disruption and harm is cause for concern" (Grabowsky and Smith as cited by Levi, 2001: 50). The situation in Canada is slightly different, as Canada has not experienced large scale terrorist attacks. Institutions appear to assume that citizens are hesitant to accept they may be at danger from terrorist attacks, therefore links between terrorists, computer crimes, and identity theft are tenuous at best. In order to convince the public that they are at risk (be it from terrorists or not) Canadian law enforcement is geared at measuring the occurrence and effects of identity theft and attempting to prove statistically that identity theft threatens citizens' wallets.

The FBI's focus on terrorism in the context of identity theft is telling when combined with FBI slippages in defining identity theft. According to the FBI, identity theft occurs "when someone assumes your identity to perform a fraud or other criminal act" (Federal Bureau of Investigation, n.d.-a), yet criminal acts outside of this definition are consistently referred to as cases of identity theft. For example, in the document "Protecting Yourself Against Identity Theft? Sometimes That's Not Enough", the crime in question is "sending e-mail blasts of advertisements…to targeted customers in massive spamming campaigns…[and] selling customer lists to other companies and falsifying their demographics" (Federal Bureau of Investigation, 2004c). Regardless of how large a problem they might be, spamming and selling marketing profiles do not fit under the rubric of identity theft. Even claims about cyberterrorism are tenuous. For

instance, the FBI's Congressional Testimony on Cyber Terrorism (a lecture on the extent of cybercrime given to a Senate Subcommittee on Terrorism, Technology, and Homeland Security) admits that not one incident referred to in the lecture comprises an actual case of cyberterrorism, but they serve as "an indication of the ability of individuals to gain access to our networked systems and the possible damage that can result" (Lourdeau, 2004). These examples include a simple bomb destroying a terminal at a hydroelectric dam, a juvenile accessing the telephone system and disrupting service to the local fire department and airport, and a group of Romanian hackers gaining access to the server of National Science Foundation's South Pole Research Station and threatening to sell the hacked information to other countries. If the FBI can provide only tenuous examples and unsubstantiated rumors connecting cybercrime to terrorism, it seems that the posited link between cyberterrorism and identity theft is largely unsubstantiated.

These slippages in defining identity theft (as well as cyberterrorism) may have a number of possible causes. Claims-making about the link between terrorism and identity theft may be rooted in efforts to inject momentum into calls for post-9/11 security increases, momentum that has been slowly declining with time and the human rights challenges evoked by initiatives such as the PATRIOT Act. Simultaneously, the FBI may be attempting to 'piggyback' anti-identity theft initiatives on the fear created by terrorism. Regardless of cause, the successful linkage of identity theft with terrorism capitalizes on the public impetus to 'do something', and garners further support (both political and financial) from the anti-terrorist agenda. Accordingly, references to both

terrorism and identity theft, and the fear they evoke are used to pattern people into the network of information exchange.

In the case of American Express, the safety/threat dichotomies can also be linked to attempts to pattern individuals into the network of information exchange. Acknowledging individual losses places security practices under suspicion and results in clientele and other corporations losing their trust in the corporation. Corporations must strike a balance between convincing consumers that a threat exists that requires the modification of one's actions and the purchase of increased security, and assuring them that consumer information, money, and patronage is safe in corporate hands. Ultimately, direct harms do not threaten businesses as much as the potential loss of reputation and trust. To elaborate:

> Consumers are becoming wary of giving out information, and are learning more about their right to privacy every day. Increasingly, they are holding organizations responsible for protections of their personnel information – not just through the law – but also through the marketplace. If businesses lose consumer confidence and goodwill, it is their bottom lines that will suffer.
>
> (Federal-Provincial-Territorial Consumer Measures Committee, 2005: 3)

Identity theft tends to be portrayed as a generalized threat that exists anywhere, one that as a matter of good business practice should be protected against. Assurances are constantly made that consumers and their personal information are generally safe when doing business with *this* particular corporation, emphasizing recent security expenditures, and money-back guarantees in the case of fraud (American Express, n.d.-a; Canadian Bankers Association, 2003a). Stipulated safety measures are presented as

extra precautions that are helpful when customers do business with *other* corporations that are less concerned about consumer safety.

To elaborate on issues introduced in chapter one, corporations—like government and law enforcement—have much to lose if customers are unwilling to divulge their personal information. For these institutions the risk of identity theft is not related to losses due to fraud, but the prospect of reticent clientele who are unwilling to divulge their information or use services and patronize companies they deem unsafe. This information is utilized to formulate user profiles that are vital to the efficient operation of virtually every institution. For example, government agencies constantly attempt to separate those eligible to receive benefits from those ineligible, and those applying legitimately from those applying illegitimately. Without citizens willing to provide information about themselves, it is difficult to detect falsified incomes, living circumstances, and identities, as detection increasingly depends on the triangulation and comparison of various information databases. Moreover, corruption of data and false or misleading information can throw the whole fragile system into disarray, because in order for risk assessments to work properly they must first be attached to accurate identities (Lyon, 2001: 296). This is a substantial issue; in Canada, stolen and falsified personal information is reportedly being used to obtain government benefits in nearly one quarter (24%) of identity theft cases (Consumer Measures Committee, 2005: 5).

Plausibly, in order to increase consumer safety, institutions require permission to access more and more of consumers' personal information—including, as in the case of Amex, their credit report and daily spending patterns. This information purportedly will allow institutions to differentiate between who is accessing systems legitimately and

who is not, thus providing commercial enterprises with a policing function (perhaps even more important than the public police). Informational profiles are used for more than just marketing and routine decisions. These reams of information are now incorporated into security measures. For instance, "business service providers may also rely upon the pattern recognition features of data mining programs to determine whether a credit card is likely to have been stolen" (Gandy, 2003: 30). An example is the data-mining techniques that allow American Express to identify with statistical certainty where Cardmember data was compromised before the start of a fraud episode (American Express, 2004b). These techniques are then used to apportion out blame for losses. If American Express determines that an unacceptable amount of fraud is located at a specific merchant site, this merchant can be held responsible for any financial losses suffered by Amex (American Express, n.d.-a). Merchants are not the only ones who warrant such information security measures. American Express also researches "Cardmember spending patterns to help identify whether the claim is legitimate" and refuses to reimburse charges they deem as customer fraud (American Express, n.d.-a). Importantly, it is corporations rather than courts that differentiate between legitimate claims and fraud, thus becoming a model of private justice.

For institutions, the solution to the 'risk' of identity theft is *not* a public wariness about dependence on documentary identity, but is in fact the opposite—an increased reliance on documentary identity in attempt to verify such identities. Information needs to be more detailed than in the past, including detailed scrutiny of such things as spending patterns, social security numbers, and phone numbers, which are touted as *the* means to verify legitimate system users and reduce identity theft. Accordingly, security

measures are increasingly elaborate and intrusive, and in the process expose more valuable information to potential thieves, thus paradoxically creating more opportunities for offences. Hence, it seems that as security measures increase, so too will the occurrence of identity theft.

In this section, examples from both the corporate world and law enforcement have shown how institutions are rife with contradictions. Emphasizing the harm of identity theft is essential in order to amass public support for anti-identity theft agendas and encourage the purchase of security measures and the uptake of protective precautions. At the same time, the emphasis on harm is moderated by assurances of some degree of safety as long as citizens follow institutional safety recommendations. These assurances help strike a balance, persuading individuals not to pull away from the system of information exchange.

Magnanimity/Self Interest

By selling security measures and publicizing prevention guidelines, institutions not only propagate conditions conducive to identity theft (e.g. the circulation and dependence upon more personal information), they do so under the auspice of altruism. Often this altruism and magnanimity is a façade for a more deep-rooted self-interest. Institutions rely on 'educating' consumers how to reduce the risk of identity theft, and in doing so disguise their own inability, or unwillingness, to eradicate identity theft. This 'education' is purportedly selflessly done by institutions eager to look after the best interests of their clients. Promoted risk reduction measures range from purchasing extra security, to increasing monitoring of data doubles by scrutinizing financial statements

and credit reports. These measures also forge a tighter relationship between customer and institution, drawing the institution into consumers' daily life.

Educating consumers about identity theft and possible risk reduction methods is undertaken not only as a free public service, it also encourages protection measures that promote the wellbeing of the institution. For example, providing corporations with more detailed personal information such as changes in address, telephone number or email, helps prevent fraud and separate identity thieves from legitimate customers, but it is also used to update user profiles. By promoting individual responsibilization, institutions circumvent some of their institutional responsibility. Moreover, many promoted protection measures serve the double purpose of gathering data used to fuel the network of information capitalism. The risk management behaviours endorsed by institutions encourage individuals to practice self-surveillance and self-reporting, and in doing so, institutions avoid expending resources and effort to surveil and collect this information themselves. Although the theme of self-surveillance is prominent in the following chapter, examples such as urging individuals to check all financial statements monthly and to purchase frequent credit reports clearly illustrates the tension between self-interest and magnanimity. Once again, it must be stressed that none of these protection schemes *prevent* or even *reduce* the likelihood of victimization, at best they can only lessen the extent of the victimization after it has occurred by responding to it quickly and reducing some of the inconveniences of the reporting process.

Even government agencies, which labour to create and maintain the image of providers of practical unbiased information, harbor motivations that are not always selfless. According to Oscar Gandy, citizens exist within 'cybernetic capitalism' -a

totalizing commercial system that depends on the ability of state and corporate bureaucracies to collect, process, and share massive amounts of personal information to track, command, coordinate, and regulate people to a remarkable extent (Gandy, 1993). As referred to in the previous section, misuse of information becomes a paramount issue given that accurate tracking, coordination and control all rest on the veracity of personal information. By providing detailed data on how to prevent and respond to identity theft, government authorities ensure the integrity of the data they depend on for their day to day operations, e.g. insurance and health benefits, taxation schemes, etc., and also convince consumers to take over protecting data under the guise of empowerment. An example of this 'empowerment' can be found in FTC documents where institutionally desired data protection measures are couched in the language of legal rights and freedoms, e.g. "You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file"(Federal Trade Commission, n.d.-c), and "[M]ost victims can resolve their cases by being assertive, organized and knowledgeable about their legal rights" (Federal Trade Commission, 2005g: 12).

Although institutional responses to identity theft often coincide with the best interests of their clientele, this is not always the case. An anecdote provided by Edmonton Police Service Detective David Vicen at a fraud awareness seminar on March 29, 2006 exemplifies this. CitiBank introduced credit cards that included photo identification and could substantially reduce identity theft, but found that a large number of female users disliked showing their picture for every purchase. Because CitiBank could lose business to credit card companies which do not require photos, the cards were never made mandatory. Often the quest for profits overrides the quest for security as

increased security measures equate to decreased profit margins. Conversely, for every occurrence of identity theft that may cost institutions money, there is also the opportunity for profit. American Express is a paradigm example of how corporate management of the identity theft threat can transform potential losses into profit. Amex's "Fraud Protection Guarantee" makes numerous assurances that if any Amex cardholder falls prey to identity theft the cardholder will not be held liable for any fraudulent charges or deductibles (American Express, n.d.-a). This prominently marketed guarantee is the first and most prominent greeting for visitors to American Express' fraud protection web pages (American Express, n.d.-e). Of course, Amex still sells two types of insurance against identity theft: CreditSecure is sold for $9.99/month or $99.95/year, whereas Identity Protection is sold for $5.95/month or $59.95/year. The two products are not mutually exclusive and cardholders may purchase both to ensure maximum protection. In fact, the two coverages are promoted as working best in concert, as Identity Protection offers enhanced financial coverage and CreditSecure offers daily credit report monitoring in order to quickly identify and act upon any suspicious activity. The credit bureau Equifax monitors the credit reports every business day and includes email notification of any suspicious activity and quarterly updates from all three major credit bureaus: Equifax, TransUnion, and Experian, which are amalgamated into a single profile (American Express, n.d.-b, n.d.-d). This monitoring lets Cardholders—and Amex—know "when someone looks at your credit profile, when an account is opened in your name, or when a new address is reported to the credit reporting agency" (American Express, n.d.-c). Permitting daily monitoring is just one example of the self-surveillance that plays a major role in the following chapter.

The differences between the two types of insurance are relatively small. Although CreditSecure offers compensation for expenses incurred while re-establishing one's 'good name', this compensation is not all-inclusive:

> CreditSecure's Identity Theft Expense Coverage reimburses victims of identity theft for certain expenses up to $5,000 (after a $250 deductible).
> Expenses covered include:
> - Lost wages as a result of time taken off from work to deal with a fraudulent incident, up to $500 per week for a maximum of four weeks. (Lost wages must occur during the policy period.)
> - Notary and certified mailing expenses for completing and delivering fraud affidavits
> - Loan application fees for re-applying for loans which were declined due to erroneous credit information that had reflected identity theft
> - Long distance phone charges associated with re-establishing your identity
> - Attorney fees incurred (with prior consent) for defending suits brought incorrectly by merchants and their collection agencies and removing criminal or civil judgments wrongly entered against the victim
>
> (American Express, n.d.-c)

In comparison, American Express' Identity Protection, only has a $100 deductible and includes the following benefits:

> Coverage of up to $15,000 including:
> - Up to $5,000 for attorney's fees and court costs resulting from legal suits or proceedings to remove judgments wrongfully entered as a result of identity theft.
> - Up to $2,000 for lost wages resulting from efforts to amend or rectify personal records.
> - Up to $2,500 restitution for fraudulent fund withdrawals from financial or credit accounts.
> -Miscellaneous fees and charges including notary services, long distance calls, postage and document copying.
>
> Access to identity theft counselors to:
> - Provide overview and examples of identity theft.
> - Outline tips and techniques Cardmembers can follow to avoid becoming a victim.

> - Help file police reports if a Cardmember is a victim of identity theft.
> - Assist with reviewing credit reports and contacting the three major credit bureaus. Provide sample dispute letters and forms to help correct inaccuracies.
>
> (American Express, 2004a)

Although the CreditSecure and Identity Protection coverages are similar in scope, each offers seemingly indispensable services for those concerned about identity theft: CreditSecure's credit monitoring and Identity Protection's 'identity theft counselors' and financial coverage. Consumers are encouraged to purchase both products, despite the Fraud Protection Guarantee, in order to secure their identity. In addition to identity theft insurance, customers are advised to sign up for 'account alerts' which use email, mobile phones, pagers and PDAs to notify customers when payment is due, when irregular account activity is detected, and when customers approach their line of credit limit (American Express, n.d.-h). These 'alerts' are yet another security measure that relies on scrutiny of information profiles.

As shown by the above examples, ideal responses to identity theft largely involve the increased monitoring of information profiles. Although customers seemingly benefit from 'education' about responsibilization methods and consent to increased monitoring by supposedly magnanimous institutions, there is also room for institutional profit. Put simply, customers pay for the privilege of having institutions monitor their behaviour, and are paying two-fold: once financially and again in terms of reduced privacy. Whether institutions are competent enough to protect these profiles from criminals is an open question.

Competence/Incompetence

The tension between institutional claims to deal with personal information in a safe and secure manner, and their past inability to protect this information indicates the difficulty in ensuring secure information networks. On one hand institutions are represented as competent and knowledgeable guides, selflessly offering assistance and recommendations that allow individuals to protect themselves from those profiting from other's identities and thereby corrupting the 'access keys' (e.g. credit card accounts, credit profiles, etc.) that are vital for interacting with the world. Yet, these same institutions often appear incompetent, unable to protect clientele and their information and incapable of efficiently rectifying matters when something goes wrong. Their ineptitude results in less reputable actants gaining this information, and also results in victims of identity theft being re-victimized by the bureaucratic red tape hindering attempts to regain their 'lost' identity. [7] At their worst, organizations are complicit in the identity theft process, continuing to trade and profit from clientele's information and fears, neglecting the expense of complete data protection and thereby making data easily accessible to thieves.

As chapter one has shown, ASTEs encourage environments conducive to identity theft by valuing depersonalized interactions based on flows of information. Although efficient, the information in these interactions is susceptible to being hijacked and illegitimately deployed. Due to the mechanics of information capitalism and current communication technology, some 'leakage' of information is expected, and institutional policies and practices dealing with the collection, handling, transfer, and storage of this information are seen as a way to minimize 'leakages'. But when these policies and

practices contribute to criminal opportunities, institutions avoid responsibility. For example, credit card fraud accounts for a significant proportion of identity theft. "Statistics gathered by PhoneBusters in 2003 and the first half of 2004 indicate the largest number of complaints surrounding identity theft relate to credit cards or false application for a credit card (32 percent)…[and] the FTC reports that in 2003, 33 percent of identity theft victims reported that their identifying information was used for credit card fraud" (Bi-national Working Group on Cross-Border Mass Marketing Fraud, 2004). Credit card companies like American Express recognize that:

> Identity thieves have been known to 'dumpster dive' to obtain documents with personal information that have been discarded…[as well as] obtain personal information by collecting individual's mail…The perpetrator then uses the information to apply for loans, credit cards, etc. The perpetrator then charges large amounts to the credit cards.
> (American Express, 2005b)

But *not once* do they directly acknowledge the linkage between the unsolicited credit applications they mail out and increasing amounts of credit card fraud and identity theft. This refusal to acknowledge dangerous institutional processes is linked to the theme of inaction, in so far as institutions choose not to abandon business practices that promote identity theft, and instead focus on tips reacting to the inevitable occurrence of this theft. As an interesting side-note, the determination of who receives mail-outs is generally based on financial information from credit reports, the very same credit reports American Express is paid to monitor by worried clients. The *Fair Credit Reporting Act* (FCRA) regulates credit reports in the United States and states that "target marketing – making unsolicited mailing or telephone calls to consumers based on information from a consumer report – is generally not a permissible purpose", yet for some unarticulated

---

[7] This re-victimization will be explicated more fully in chapter three.

reason, credit and insurance offers are exempt from this rule (Federal Trade Commission, 2005f: 8). While American Express is charging to monitor customers' credit reports, it is simultaneously using these reports to select individuals to receive credit offers, which in turn are targeted by potential identity thieves.

Of all the actors comprising this research, government agencies are alone in recognizing that perpetrators of identity theft are often trusted insiders—employees with 'legitimate' database access rather than tech-savvy hackers. This seems like a forthright recognition of the facts, and a refreshing willingness to accept blame instead of deflecting it onto unknown criminal Others. But recognition of 'insider jobs' is unsurprising given the number government and corporate employees who have access to confidential databanks. There are bound to be information leaks within national health, education, and insurance networks of such magnitude. Yet, "[t]he protection of personal information stored on our nation's computer systems is critical to public trust in those networks and the health of our economy"(Federal Bureau of Investigation, 2004c).

Recognizing that vital government systems are infiltrated by identity thieves puts into question the security of the whole network, and can lessen public trust in the competence of both the system and the government. When an information breach occurs that cannot be hidden, it is beneficial to blame this breach on a dishonest employee rather than on flaws inherent to the system itself. Accepting some responsibility for 'wayward' employees and promising to watch them more closely becomes a tactic to avoid institutional liability. By acknowledging that dishonest or incompetent employees who do not follow privacy guidelines are to blame for security

breeches, public attention is focused on individual perpetrators rather than systemic failures and criminogenic conditions.

Surprisingly, other institutions are loathe to admit to insider crime problems, and government agencies are the first to recognize that perpetrators are likely dishonest employees leaking information for their individual gain. This is supported by up to 70% of identity theft being traced to leaks that occur within organizations, rather than outside infiltrators (Collins as cited by Consumer Measures Committee, 2005: 6; Jewkes, 2002). According to government discourse, although employers take measures to ensure that privacy policies are understood and only reputable persons hired, a few individual employees who leak information are to be expected (Federal-Provincial-Territorial Consumer Measures Committee, 2005).

More often, information leaks—when they cannot be blamed on corrupt individuals—are blamed on the incompetence of other institutions. For example, while government agencies persuade citizens to provide more detailed knowledge about themselves to government sources in order to secure against and investigate identity theft, these agencies advocate taking advantage of an "'opt-out' choice that limits the information shared with others" (Federal Trade Commission, 2003b). Citizens can then opt-out of pre-approved credit offers, telemarketing mail, e-mail, and telephone solicitations. Here, other institutions are depicted as incompetent at protecting personal information and customers are warned away from commercial information gathering attempts: "Don't fill in forms for contests, rebates or draws that ask for more information than what you are prepared to give. This information could be sold to a telemarketer, or to others with criminal purposes in mind" (Alberta Government

Services, 2004: 3). Warnings like these equate telemarketers to criminals, and in doing so, draw the line between businesses who needlessly demand information and the government who requires this information in order to extend services and benefits. Interestingly enough, these warnings serve to 'blacklist' longstanding legal and legitimate business practices such as consumer loyalty cards, coupons, rebates, contests and warranty forms. It seems that putting one's name, telephone number, and address in 'giveaway' draws is now a security risk that places one's identity, credit rating and financial accounts in danger. Ultimately, consumers are cautioned to be wary of placing their trust and personal security in the hands of corporations who may be more interested in profits than confidentiality.

Although allegations of incompetence and accusations of blame are commonplace, institutional silence about concrete causes of identity theft and sure-fire solutions has largely prevailed. The CBA states that identity theft "is the fastest growing and most serious crime in North America aimed at consumers. This is largely due to the development of new technologies such as 'card-skimming'[8] devices and to criminal involvement in computer hacking" (Canadian Bankers Association, 2003b: 1). As such, the CBA warns customers about the dangers of doing business on the internet. These warnings include exhortations to "Be skeptical" as well as "Use common sense and be aware of potential security leaks....Use caution...[and] be suspicious" (Canadian Bankers Association, 2005a, 2005c). Abstract cautions such as these are largely pointless exercises that risk undermining trust. Conversely, while warning customers

[8] Card-skimming refers to when employees take second copies of credit and debit card details from customers' cards' magnetic strips before 'legitimately' processing the payment.

away from internet banking, CBA schizophrenically continues to lure customers *toward* internet banking, itself one of the institutional preconditions for such fraud:

> Customers access online banking services for routine transactions and for a growing list of credit and investment services – mortgages, car loans, small business loans, mutual funds, and securities purchases. Most major banks now offer mobile banking services through digital cell phones and other wireless devices. Wireless banking services include reviewing recent transactions, retail and investment account balances, and paying bills. Customers are also able to transfer funds from their account to the account of another person at another bank using e-mail to send instructions.
>
> (Canadian Bankers Association, 2004a: 28)

Lamenting the technology that empowers "criminal involvement in computer hacking" directly contrasts with increased reliance on this same technology for routine banking purposes. The banking industry never acknowledges that practices such as using cell phones or e-mails to access funds are preconditions for 'identity thieves'. This schizophrenic attitude is also evident in terms of credit card usage. For example, in the same document that the FBI warns not to give out credit card numbers online, they state that "The safest way to purchase items via the Internet is by credit card because you can often dispute the charges if something is wrong" (Federal Bureau of Investigation, n.d.-b).

Even more worrying than the realization that institutions' informational practices are seriously implicated in identity theft is the realization that institutions may be incompetent to halt the criminogenic process they have fostered. Institutions, in an effort to induce individual responsibilization, constantly stress the inability of law enforcement, government, and business to effectively combat identity theft. This is achieved by emphasizing characteristics that make identity theft different from other

crimes, the most important being the reliance on technology, which has been alluded to multiple times earlier in this paper.

Normally the first line of defense against crime, law enforcement agencies readily admit that identity theft cannot be entirely prevented. As stated by the FBI, "The sources of information about you are so numerous that you cannot prevent the theft of your identity. But you can minimize your risk of loss by following a few simple hints" (Federal Bureau of Investigation, n.d.-a). This statement is closely echoed by Phonebusters: "While you probably can't prevent identity theft entirely, you can minimize your risk. Identity theft is on the rise and it can happen to anyone. It can happen to you" (PhoneBusters, n.d.-c). Declarations such as these serve to remind the public that policing cybercrimes is something the police cannot do on their own.

As was introduced in the Action/Inaction section, in every research site except for the FBI, there is a commonality: the general lack of a perpetrator profile. Instead of being a victimless crime, identity theft seems to be an offenderless crime wherein a criminal profile is largely absent. This is somewhat surprising given the perception that offenders are omnipresent as evidenced by the claim that "[i]dentity theft is committed in every place associated with daily life" (Bi-national Working Group on Cross-Border Mass Marketing Fraud, 2004: 2). This anonymous omnipresence is largely due to communications technology that allows offenders to be anywhere that computers are—and thus everywhere. Lurking in cyber networks, offenders are faceless perpetrators constrained neither by time nor space. Crimes over the internet happen instantly, regardless of whether the victim is two hundred feet away or two thousand kilometers away. These criminals are portrayed as appearing from nowhere and disappearing as

quickly as they came, they are fluid creatures whose presence and trespass seemingly cannot be predicted or traced, let alone avoided and controlled (Bauman, 2002).

Several authors have recognized that the reputed technological aspect of identity theft poses many obstacles to its control, especially in the context of law enforcement (Chan, 2001; Finch, 2002; Jewkes, 2002; Wall, 2001, 2002). One important attribute is police culture which is traditionally conservative. Officers may be unfamiliar or unwilling to work with the computer forensic practices needed to trace criminal transactions and target offenders over the internet because this "office work" goes beyond established perceptions of what police work entails. Even if officers have the skills and desire to police the internet, entire departmental budgets can be consumed without affecting the vast number of internet infractions. Furthermore, identity theft committed via the internet hinders investigation of offenders because they may be located thousands of miles from both the victim and the law enforcement agency investigating the theft. The internet's global reach and pliancy allows evasion of authority since criminals hide in anonymity or retreat beyond the bounds of their jurisdictions, knowing that police are reluctant to cross territorial lines (National White Collar Crime Center & Federal Bureau of Investigation, 2005: 13).

Even if an offender is located by the authorities, prosecution is exceedingly difficult. Often with cases of identity theft there are no reference points in law and so the 'offence' may not be an actual crime as defined by the Criminal Code of the country in which it occurs. Even if the harm is categorized as a criminal offence, prosecution is still difficult, time consuming, and expensive. Law enforcement agencies are faced with growing complaints about a crime they can do little about. Determining if an actual

crime has occurred, investigating the matter, pinpointing a criminal and finally prosecuting the criminal are inefficient and expensive methods that depend on resources that law enforcement does not have.

Even reporting identity theft and other crimes committed over the Internet is problematic. Victims may be unaware of their victimization, too embarrassed or ignorant of what to do, or they may shrug it off as a learning experience, especially if the harm is minor. For example, according to the FTC's Identity Theft Data Clearinghouse, in 2004, 61% of those aware that they are victims of identity theft did not notify the police (Federal Trade Commission, 2005d: 11). The National White Collar Crime Center also recognizes the challenges associated with reporting identity theft, "research indicates that only one in ten incidents of fraud ever make their way to the attention of enforcement or regulatory agencies (National White Collar Crime Center & Federal Bureau of Investigation, 2005: 17).

Accordingly, the difficulties associated with reporting identity theft creates problems for those attempting to discover the extent of identity theft victimization, resulting in conflicting reports about the extent of the crime. For example, American Express in its document entitled *Identity Theft Assistance: Safeguarding Your Identity* states that "[t]here are between 500,000 – 750,000 victims per year" (American Express, 2005c: 2), yet on a webpage detailing the benefits of purchasing CreditSecure, they claim that "[i]dentity theft is one of the fastest growing crimes in the U.S., with nearly 10 million incidents last year" (American Express, n.d.-c). Granted, the former statistic details the number of victims while the latter quantifies incidents, but each victim reporting up to 20 different victimizations in one year does not seem likely.

Inconsistencies in reporting the extent of identity theft victimization as well as the amount of financial harm are not restricted to American Express. Conflicting dollar amounts and victimization rates are found within the Canadian Bankers Association, the RCMP, and SafeCanada as well (Bi-national Working Group on Cross-Border Mass Marketing Fraud, 2004; Canadian Bankers Association, 2003a, 2003b; PhoneBusters, n.d.-b; Royal Canadian Mounted Police, 2004; Solicitor General Canada, n.d.). With these discrepancies in mind, one can draw three conclusions: 1) institutions are incompetent to the point that they cannot even estimate the extent of the danger without contradiction, 2) institutions are intentionally misrepresenting statistics and are grossly inflating the prevalence of identity theft in order to encourage certain types of consumer behaviour, or 3) identity theft is so nebulously defined and fluid that it is near impossible to count.

The above examples show how admitting inability to respond effectively to identity theft can be used to the benefit of institutions. Claims that institutions alone are incapable of eradicating identity theft are used as a tactic to avoid responsibility for the criminogenic conditions institutions create, to shift blame to others (both individuals and other institutions), and explain away any incompetence in responding to identity theft.

Attending to the tensions and the contradictions that are present within the four axes detailed in this chapter, 1) safety/threat, 2) action/inaction, 3) magnanimity/self-interest, and 4) competence/incompetence, reveals a common thread. Each of the inconsistencies detailed above accommodate the dictates of both the information network and the institutional actants who seemingly control this network. These inconsistencies are used to the advantage of institutions, protecting and perpetuating the

flows of information that have become their lifeblood, (e.g. linking safety precautions to divulging—rather than withholding—personal information). Ultimately, institutions use their purported failures (i.e. inability to protect all information), to strengthen governance-at-a-distance. Although institutions are admittedly weak in personally preventing and responding to identity theft, they are seen as the best purveyors of 'sound' advice and protective devices. Thus institutions assume a directorship function: broadcasting knowledge and guidelines, and ultimately downloading security labour and responsibility for protection onto individuals themselves.

Chapter Three: Forging the Hyper-Vigilant Subject

DON'T LET THIS HAPPEN TO YOU!
How to Protect Your Good Name from Identity Theft

> Are collection agencies suddenly demanding payment for items you've never bought? Have you stopped getting your credit card and bank statements in the mail? Are stores refusing your checks claiming you have a history of bouncing them, even though you don't?
>
> **You may be a victim of identity theft.**
>
> Identity theft is one of the fastest growing crimes in the U.S., claiming more than 10 million victims a year. The FBI is working with its partners—private sector companies, regulatory agencies, and other law enforcement organizations—to curb identity fraud…But you can help us—and more importantly, help yourself—by taking some basic preventative steps.
>
> (Federal Bureau of Investigation, 2004b)
>
> Identity theft victims may spend years—and large sums of money—restoring their credit histories and their good names. Some consumers have been denied jobs or insurance or been arrested for crimes they did not commit.
>
> (Federal Trade Commission, 2005c)

This chapter is directed along the following trajectory: institutional discourses, often composed of alarmist excerpts like the ones above, encourage individuals to responsibilize themselves in order to protect against identity theft. Recommended responsibilization efforts initiate individuals, who are seen as the 'weak link' in the system of information exchange, into a realm of intense surveillance. Fueled by an institutional documentary frenzy, citizens and victims are increasingly subjected to myriad informational demands, all of which serve to pattern this 'weak link' into shoring up the informational system. These demands encourage the formation of a late

modern hyper-vigilant subject whose range of response both to crimes and institutions is severely limited. Ultimately, for victims, much of the harm of 'identity theft' is generated by institutions and their surveillant practices, not thieves.

Actor-Network Theory (ANT) is useful in conceptualizing the network of information exchange and institutional demands for increased responsibilization and surveillance (Latour, 2004, 2005; Law, 1992; Law & Hassard, 1999). Many discrete elements, both animate and inanimate, compose the informational network, including law enforcement, consumer protection agencies, businesses, individuals, pamphlets, 'hackers', credit cards, identification documents, electronic databases, computers and other Automated Socio-Technical Environments (ASTEs). These elements, termed actants, do not share the same trajectories, influences, or goals, and as such the informational system is situated in a networked struggle to make them operate in a coordinated fashion, with constant resistance and reshaping of its composition.

In order for the network to stabilize, actants are pressured by other, more organized, actants to behave in ways that are amenable to the continued operation of the network. In this case, institutions have their own conception of what the information network should be used for and how it should be maintained. They thus pressure other actants to help create and perpetuate their ideal system. ASTEs, as will be seen in this chapter, are vital to the process of patterning recalcitrant nodes into the information network. Murdoch gives a cogent summarization of this process:

> In order for an actor successfully to enroll entities (human and nonhuman) within a network, their behaviour must be stabilised and channelled in the direction desired by the enrolling actor. This will entail redefining the roles of the actors and entities as they come into alignment, such that they come to gain new identities or attributes within the

> network. It is the intermediaries ... which act to bind actors together, 'cementing' the links. When there is a perfect translation, or redefinition, of actors' identities and behaviours then these are stabilised within the network. The stronger the network, the more tightly the various entities (human and nonhuman) are tied in.
>
> (cited by Haggerty, 2001: 61)

'Unruly' actants (i.e. individual consumers who may be reticent with their information) are reigned in by intermediaries (i.e. ASTEs) and more organized actants (i.e. institutions) who play off individuals' desires, needs, and fears to pattern their behaviour in a particular direction.

Institutions strengthen and stabilize conceptions of identity theft as a threat, and in doing so use responsibilization measures and surveillance to further link individual actors into the network of information exchange. Individuals face institutional processes of patterning and social orchestration in the endeavor to shape and transform them so they assume roles beneficial to the functioning of the knowledge network. Being that the network is only as strong as it weakest point, individuals are pressured to work in a certain way, to release certain information, at a certain time, in certain amounts, in a certain order, to specifically preferred actors, in a manner that ensures the stability of the whole informational system. In doing so, subjects are made more visible to the institutional gaze.

Institutional techniques aimed at stabilizing the information network ultimately foster a hyper-vigilant subject who is attentive to the risks associated with identity theft and the misuse of personal information. Paradoxically, these techniques stabilize the network and limit resistance, but in tying subjects so tightly into the system, institutions have rendered subjects largely impotent to prevent identity theft. Responsibilization

methods that are unquestioningly accepted by individuals as means of protection from 'identity thieves', are used by institutions to externalize tremendous amounts of security labour onto individuals.

Rationalization supporting responsibilization and individual security efforts in lieu of institutional efforts is often broached in technological terms. ICT channels necessary for commerce and governance carry flows of information relating to identity, so precision is desired in every transfer of information over the internet. But these channels are so porous that cyberspace can never be secure (Lyon, 2001), as suggested by the following quote:

> Once information is collected, is can be used, shared—and possibly abused—in countless ways. It can be difficult to determine what happens to personal information circulating on the Internet. Media stories about hackers gaining access to supposedly secure Web sites and obtaining credit card numbers and other personal information suggest that few, if any, Web sites are completely secure. Poor information handling and security practices may cause risks to your privacy by allowing unauthorized access. So may the dishonest or disgruntled insider who has legitimate access to your information but uses it fraudulently.
>
> (Office of the Privacy Commissioner of Canada, 2003)

There are seemingly insurmountable difficulties involved with policing ICT channels and ensuring information security, yet "the notion of insecure computer networks is literally untenable for the powers that be in our world - everything depends on these networks, and control over these networks is an essential principle of remaining in control" (Castells, 2001: 177). In this context, mediating the occurrence of identity theft has more to do with reducing the number of suitable targets than with reducing the number of motivated offenders.

As argued in the previous chapter, despite their best efforts, institutions cannot guarantee complete security—especially when it comes to the internet, which is commonly seen as lawless and chaotic. Responsibilization discourses are thus marketed as a way to 'empower' individual actors. Through responsibilization, and the marketing of security measures such as identity theft insurance and computer firewalls, actors are able to temporarily find comfort, reassurance, and order, and to see the world as stable, coherent, and manageable, despite the recognition that the state cannot protect them from all harm.

Commonly, risk management techniques take the guise of instructions to prevent identity theft. These instructions are all similar, regardless of whether the 'tips' come from government, law enforcement, or business. The following are found within every research site:

- Before you reveal any personal information, find out how it will be used and if it will be shared.
- Pay attention to your billing cycles. Follow up with creditors if your bills don't arrive on time.
- Utilize passwords on your credit card, bank and phone accounts. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SIN or your phone number. Do not give out or allow anyone to see your password or PIN number.[9]
- Minimize the identification information and number of cards you carry.
- Do not give out personal information on the phone, through mail or over the Internet unless you have initiated the contact or know with whom you're dealing.
- Keep items with personal information in a safe place. An identity thief will pick through your garbage or recycling bins. Be sure to tear or shred receipts, copies of credit applications, insurance forms, physician statements and credit offers you get in the mail.

[9] Although American Express does not explicitly advocate putting passwords on credit card accounts, they do advocate safeguarding any account numbers and PIN numbers one may have (American Express, 2005a).

- Give your Social Insurance Number (SIN) only when absolutely necessary. Ask to use other types of identification when possible.
- Don't carry your SIN card; leave it in a secure place.

(American Express, 2003, 2005a, 2005c; Canadian Bankers Association, 2005b; Federal Bureau of Investigation, 2004b, n.d.; Federal Trade Commission, 2005g; PhoneBusters, n.d.-b; Solicitor General Canada, n.d.)

Institutions also promote risk management 'tips' that are geared to *responding* to identity theft victimization rather than *preventing* it. The fact that response tips greatly outnumber prevention tips points to a tension in institutional motives, as measures responding to identity theft may serve institutional agendas better than eradicating the phenomena entirely. The procedure to follow once an individual discovers they have been victimized is relatively standardized, with institutions in this study[10] agreeing on the steps as follows:

1. Contact the Police and file a report. This report becomes vital later on when proving your victimization to the Credit Bureaus, Account Providers, and Government Authorities.
2. Contact the three major Credit Bureaus to review your credit report for any discrepancies and register a fraud alert.
3. Notify your financial organizations and close the accounts you know or suspect involve identity theft.
4. Contact the Government Authorities in order to log your complaint and provide statistical information to the relevant authority (i.e., PhoneBusters, FTC) as well as contacting the agencies that issued identification, such as your driver's license or Social Insurance number, you suspect has been tampered with.

(American Express, 2005b; Consumer Measures Committee, 2004; Federal Bureau of Investigation, 2004b; Federal Trade Commission, 2005g; PhoneBusters, n.d.-a)

The quest for security is highly commodified and as such works to *undermine* feelings of security by inculcating anxiety through advertising campaigns and 'special'

[10] This is with the exception of the Canadian Bankers Association which does not include any information about how to proceed once victimized.

reports which emphasize the risks of identity theft and promote 'solutions' available for purchase. The most common solution is increased surveillance of citizens. In order to manage risk—but not eliminate it—increasingly precise knowledge is sought. A typical example of this knowledge is when businesses rely upon the pattern recognition features of data mining programs to determine whether a credit card is likely to have been stolen (Gandy, 2003: 30). Increased knowledge about protection from risk reveals further risks and areas of insecurity, thus this knowledge perpetuates, rather than eliminates, risk (Ericson & Haggerty, 1997).

Paradoxically, institutionally mandated responses to identity theft result in the circulation of more and more personal information rather than limiting its volume. This situates individuals into a remarkable regime of documentation predicated on technologies of governance such as increased surveillance. The drive for surveillance is fuelled by the belief that surveillance is synonymous with control, and "if surveillance is thorough enough then disturbances can be anticipated and dealt with" (Ball & Webster, 2003: 14). Institutions promote amplified surveillance in terms of consumer protection by equating increased surveillance to decreased opportunities for identity theft and other crimes. Surveillance is employed to ensure that citizens remain within the boundaries of the law, but it is also used strategically by institutions in order to learn about clientele and make operational decisions.

To separate criminals from the law abiding, all are subjected to the panoptic gaze. A widening net surveils all users of the communication technologies commonly linked to identity theft, such as the internet. This net, or more accurately, this surveillant assemblage (Haggerty & Ericson, 2000) co-exists with the desire to create data doubles

that will predictably enable better governance and commerce, bringing to light the paradoxical proposition that, while law enforcement and other agencies are finding it increasingly difficult to regulate the activities of criminals and deviants, 'ordinary' citizens are finding themselves subject to greater levels of electronic surveillance (Jewkes, 2002).

The reasons *why* ordinary citizens are under more intense scrutiny becomes a topic of interest. Because perpetrators largely evade the gaze of surveillance, a new subject and site for inspecting the identity theft phenomenon must be found. This subject is the victim themselves, as exemplified by the FTC databanks. The Federal Trade Commission is mandated with maintaining an Identity Theft Clearinghouse which is the sole national repository of consumer complaints relating to identity theft in the United States. Officially, the Clearinghouse provides investigative material for law enforcement, as well as providing information to both the private and public sector on trends and methods to reduce identity theft (Federal Trade Commission, 2005d). But in the absence of a targeted perpetrator, the Clearinghouse instead provides a "picture of the nature, prevalence, and trends of the identity theft *victims* who submit complaints" rather than expressly trying to gather data on possible perpetrators (emphasis added, Federal Trade Commission, 2004b: 13). Victims and *not* offenders become the object of statistics, trend predictions, risk profiling, and surveillance in general. This approach is not restricted to the FTC and the United States, and is utilized by Canadian equivalents to the Clearinghouse: the RCMP's Phonebusters and RECOL programs.

There are multiple rationales for endorsing this victim-centered approach, a few of which will now be detailed. Introducing the victim as the 'new' surveillant subject

has to do in some part with the demographic of victims themselves, as they do not fit the traditional victim profile. Victimization is not restricted to a particular geographical location, a single gender, or specific ethnic group. Victims of identity theft break the historical mold and are not generally the underclass, the impoverished, or the oppressed. The users of the internet, and thus victims of cyber-assisted crimes such as identity theft, are generally the middle to upper class that have access to technological resources. The middle to upper class are also more suitable targets for criminals because of the amount and size of their financial accounts and the associated number of credit and debit cards used in their daily lives. Although somewhat counterintuitive to traditional conceptions of crime, this profile is recognized in a 2004 report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States. This report acknowledges that "[t]he victims of identity theft come from every age group and all segments of society; however, the majority of victims appear in segments of the population with good or potentially good credit ratings" (Bi-national Working Group on Cross-Border Mass Marketing Fraud, 2004).

The middle to upper class victim profile may partially explain why identity theft is granted so much attention, as those at risk hold more societal capital and are more readily able to direct media attention and gather resources aimed at combating the identity theft threat. Those who possess power become targets because they are more heavily tied into the established network. Names, numbers and other data detailing these persons exist in numerous locations: in employment records, bank accounts, corporate documents, property titles, etc.. Every piece of personal data broadcast over communications channels creates opportunities for its misuse. In comparison, those

who lack internet access, bank accounts, and social standing are relatively safe because less electronic data exists about them, and there is little benefit in assuming their identity for financial gain.

The difficulties policing identity theft and apprehending and prosecuting 'identity thieves' that were presented in the previous chapter form another rationale for endorsing the victim-centered approach. Due to the apparent inability of law enforcement to respond to identity theft as adequately as they respond to 'traditional' crime, another approach must be taken to deal with the rising number of complaints. Victims must be assured that something is being done, especially as pleas for increased budgets and resources, both for government and law enforcement, depend on taxpayer support. This results in emphasis placed on gathering data on identity theft trends, which become the basis for rhetorical claims made about this 'major problem'. Victims are encouraged to believe their reported details are being used constructively to 'break open' a much larger case, a perception buttressed by statements like the following: "[b]y sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials across the nation track down identity thieves and stop them" (Federal Trade Commission, 2005g: 8). Simultaneously, exhortations throughout the process state that "due to the nature of the crime, police can determine very little from one incident. They need to see it in context and need additional forensic evidence…that an individual client cannot provide" (Canadian Bankers Association, 2004b: 12). This generates the expectation that although the police are working diligently, results will not be immediate and are not

guaranteed. Victims of identity theft become the primary unit of analysis and object of surveillance.

The new position that real and potential victims occupy in the panoptic gaze can be linked to Actor Network Theory, which was introduced earlier in the chapter. Institutions shore up weak points in information transfer through various techniques. Generally these 'weak points' are understood to be individuals who fail to signify adequately enough to placate institutional desires for information. In the context of identity theft, institutional methods range from the relatively benign—such as providing tips and resources—to the less benign—such as fostering fear or outright coercion.

When victims of 'identity thieves' report the event to authorities, coercion is used to initiate these individuals into the information network. How much and how quickly victims divulge information about themselves and the crime is portrayed as being related to whether the crime will be investigated—let alone solved—as well as whether the victims will be held financially liable for any losses. Government, business, and law enforcement use multiple techniques to ensure that victims willingly, speedily, and accurately disclose all relevant information. For example, how quickly financial institutions are notified of suspected account tampering limits liability. "If your ATM or debit card is lost or stolen, report it immediately because the amount you can be held responsible for depends on how **quickly** you report the loss." If customers wait more than 60 days to report a debit or credit card loss, they can be held completely liable for any fraudulent charges (author's emphasis, Federal Trade Commission, 2005g: 13).

Beyond such scheduled timelines, technologies of governance that tie individuals into the information network also take the shape of mandated charts and

forms to be completed by individuals. These are used to produce statistics and reduce people into data profiles. Ironically, methods to *prevent* identity theft center on protecting information, while methods to *respond* to identity theft victimization centre on creating and collecting additional information. The Identity Theft Affidavit is a telling example of this, as it is often required by victims to formally disclose information about their victimization. A standardized report that can be downloaded from multiple websites, the Affidavit asks for a host of detailed information, including but not limited to:

- Full legal name and any aliases used.
- Date of birth.
- Current address as well as any previous addresses.
- Business, home, and alternate contact numbers.
- Social Security Number.
- Driver's License number.
- Financial account numbers and details.
- Detailed information about the incident including timelines, account information, and suspicions on how the theft occurred.
- Reported losses.
- Copies of police reports as well as names or badge numbers of the officers dealt with.
- Proof of identity, such as photocopies of government issued identification.

(American Express, 2005b; Federal-Provincial-Territorial Consumer Measures Committee, 2005; Federal Trade Commission, 2005g; PhoneBusters, n.d.-a)

In its instructions accompanying the Identity Theft Affidavit the FTC states "To make certain that you do not become responsible for any debts incurred by an identity thief, you must *prove* to each of the companies where accounts were opened or used in your name that you didn't create the debt…*incorrect or incomplete information will slow the process of investigating your claim and absolving the debt*" (emphasis added, Federal Trade Commission, n.d.-b: 1). Victims must prove their innocence and are punished if information is not divulged according to institutional demands. When reporting identity

theft, the accuracy and amount of information disclosed plays a key role in ascertaining liability. Victims are influenced to reveal every detail relating to the incident—whether they regard it as relevant or not—under the threat that any omissions or inaccuracies will look suspicious. In this way, victims are cast in a role generally reserved for offenders. They become objects of suspicion and are coerced into self-reporting in order to 'prove' their innocence and absolve guilt for their own victimization.

The more information that is divulged and recorded in databases opens up additional opportunities for this information to be leaked and exploited. Yet, this further compilation of data is just what the Affidavit demands. Paradoxically, a secure informational identity means having control over one's data, but this can only be secured by an almost ritualistic revealing of every detail about oneself. Victims do not easily regain their identity: they must fight for it, winning the battle only when they willingly disclose any and all requested information. This endless cycle of disclosure is never recognized as problematic in any of the institutional literature studied.

The quest for information, plausibly in the pursuit of justice—and approved insurance claims—goes deeper than the Identity Theft Affidavit. The Affidavit is accompanied with the instructions (from every site except the FBI and CBA) to keep a log of who one talks to, their contact information, what was said, and at what time (American Express, 2005b; Consumer Measures Committee, 2004: 4; Federal Trade Commission, 2005g: 11; PhoneBusters, n.d.-a). In fact, the FTC and Amex both provide blank "Activity Logs" (American Express, 2005b: 8; Federal Trade Commission, 2005g: 11). Not only are victims encouraged to indefinitely keep all

identity theft correspondence, they are directed to send everything via costly registered mail to prove that the institution they are in contact with has received their missive.

Ultimately, the Identity Theft Affidavit serves a self-monitoring and self reporting function. It is a technology of the self wherein people are required to account for their behaviour and report on themselves to the authorities. Victims are informed that while there are no assurances that an identity theft case will be resolved or stay resolved, keeping logs and correspondence will help avoid recurring problems. For the most part these problems are not related to the crime itself or the chance of further criminal victimizations, but are specifically related to problems dealing with large organizations and bureaucracies. When responding to identity theft, institutions, just like victims, have a timeline to which they must adhere. For example, credit card companies in the United States "must resolve the dispute within two billing cycles (but not more than 90 days)" after an Affidavit is submitted (Federal Trade Commission, 2005g: 19). Activity logs are one of the few methods of holding organizations accountable for their actions, especially in relation to their handling, storage, and retrieval of data relevant to cases of identity theft. Even these institutions admit, and plan for the fact, that affidavits and documentary evidence of a victim's 'innocence' may be misplaced among the reams of information maintained by these bureaucracies, thereby returning the victim to a position of suspicion.

Once an identity theft dispute is settled with a company, victims must ask for and save any documentation stating that matters have been resolved and discharging responsibility for any fraudulent debts. "The letter is your best proof if *errors* relating to this account reappear on your credit report or you are contacted again about the

fraudulent debt" (emphasis added, Federal Trade Commission, 2005g: 7). This proof becomes another form of documentation to be protected. Bureaucratic mismanagement of case details, euphemistically termed "errors", relegates the victim back to the status of suspicious claimant. The letter is the sole token of innocence that saves the victim from having to restart the entire ordeal. To reiterate, victims here are not protecting themselves from identity theft at all, but rather from bureaucratic organizations whose mismanagement of information can result in records testifying to their innocence being lost, forcing victims to re-establish their innocence.

Repeating a theme introduced in chapter two, institutional incompetence in resolving identity theft cases seems wide-spread, and appears to be an institutional expectation, necessitating the FTC's "Tips for Organizing Your Case" to help victims:

> • Have a plan when you contact a company. Don't assume that the person you talk to will give you all the information or help you need. Prepare a list of questions to ask the representative, as well as information about your identity theft. Don't end the call until you're sure you understand everything you've been told. If you need more help, ask to speak to a supervisor.
> • Write down the name of everyone you talk to, what he or she tells you, and the date the conversation occurred. Use *Chart Your Course of Action*[11] to help you.
> • Follow up in writing with all contacts you've made on the phone or in person. Use certified mail, return receipt requested, so you can document what the company or organization received and when.
> • Keep copies of all correspondence or forms you send.
> • Keep the originals of supporting documents, like police reports and letters to and from creditors; send copies only.
> • Set up a filing system for easy access to your paperwork.
> • Keep old files even if you believe your case is closed. Once resolved, most cases stay resolved, but problems can crop up.
>
> (Federal Trade Commission, 2005g)

In this context, companies appear less benign and are seemingly not trusted to act competently in the best interests of the individual. From this perspective, true

victimization is not at the hands of 'identity thieves', but rather due to the bureaucratic labyrinth than individuals must navigate to re-establish their identity. The harm of 'identity theft' is caused by the same bureaucracy that offers to guide individuals through the victimization process for a fee. A huge onus is laid on the victim to present their 'case' in a detailed and systematic way. Resolving outstanding issues pertaining to their victimization is recognized as an arduous and time-consuming ordeal, even with institutional 'aid'.

Beyond Activity Logs and Identity Theft Affidavits, the ordeal to establish innocence becomes heightened in the event that a criminal assumes a victim's name, is apprehended, and then is charged under the victim's name. In cases such as these the line between offender and victim is further blurred, with the victim having to undergo a strikingly similar process in comparison to that of an actual criminal—except the criminal has the privilege of being considered innocent until proven guilty. Another major difference is that the victim is expected to cooperate and undergo these procedures willingly, and will be judged as wanting or failing should they not perform these tests adequately.

If wrongful criminal violations are attributed to a victim's name, (e.g. a thief, Sam, when apprehended, claims she is Chris, and thus innocent Chris is charged for the crime) the FTC advises the victim (in this case, Chris) to contact either the police or sheriff's department that originally arrested the identity thief or the court agency that issued the warrant for the arrest and file an impersonation report. To confirm their true identity the victim must:

---

[11] *Chart Your Course of Action* is the name given by the FTC to its version of an Activity Log.

> Ask the police department to take a full set of your fingerprints, photograph you, and make a copies [*sic*] of your photo identification documents, like your driver's license, passport, or travel visa. To establish your innocence, ask the police to compare the prints and photographs with those of the imposter.
> (Federal Trade Commission, 2005g: 21)

There is no reassurance that the victim's fingerprints will be destroyed and not stored indeterminately alongside those of convicted criminals instead. The victim's ordeal, however, does not end with just the fingerprinting.

> The law enforcement agency should then recall any warrants and issue a "clearance letter" or "certificate of release" (if you were arrested/booked). You'll need to keep this document with you at all times in case you're wrongly arrested again…Once your name is recorded in a criminal database, it's unlikely that it will be completely removed from the official record. Ask that the "key name" or "primary name" be changed from your name to the imposter's name, (or to "John Doe" if the imposter's true identity is not known), with your name noted as alias.
> (Federal Trade Commission, 2005g: 21)

The warning that the victim's name will most likely remain linked to the criminal (and conversely that the criminal's name will be forever linked to the victim's), at least in law enforcement files, evidences the difficulty or even impossibility of correcting misinformation in databases. More importantly, processes such as these wherein victims are not only processed, fingerprinted, and put on a criminal database but also must constantly carry proof that they are not criminals, serve to solidify the charge that victims essentially assume the 'offender' role in terms of being subjected to intense official scrutiny and mistrust.

On top of this, although institutions may sometimes fail to protect personal information and legal identity, organizations such as the FTC place ultimate

responsibility on individuals with statements such as: "If you notice that your personal information may have been compromised, taking certain steps quickly can minimize the potential for theft of your identity" (Federal Trade Commission, 2005a). Information compromises are treated as unavoidable, and avoiding damage lies not in eliminating information compromises altogether, but rather through proper individual responses such as closing tampered accounts, filing identity theft affidavits, and alerting financial institutions, government, and law enforcement. Yet, even if individuals followed every tip and recommendation given by institutions, they still would not be safe from identity theft, a fact recognized by the same institutions that are advocating responsibilization as the 'solution'. The supposed 'empowerment' granted by responsibilization is ultimately hollow as "[t]he sources of information about you are so numerous that you cannot prevent the theft of your identity." (Federal Bureau of Investigation, n.d.).

Critiquing Responsibilization

Although critique of identity theft discourses has been interspersed with much of the foregoing, the following section is devoted to a further critique of the responsibilization measures endorsed in these discourses. The foundation of this assessment lies in the previously noted fact: Individuals are unable to prevent identity theft because "as much as 70 percent of all identity theft can be traced to leaks that occur *within* organizations, such as employees who accept bribes or who pilfer customer information on behalf of organized crime." Clearly, the institutionally prescribed personal risk management techniques are unable to prevent individual victimization, as information leaks are largely due to institutional practices.

Ultimately, at the heart of matter, are the institutional efforts to avoid responsibility. There seems to be no 'crime-free' zone, given that:

> Simply by doing things that are part of everyday routine—charging dinner at a restaurant, using payment cards to purchase gasoline or rent a car, or submitting personal information to employers and various levels of government—consumers may be leaving or exposing their personal data where identity thieves can access and use it without the consumers' knowledge or permission.
>
> (Solicitor General Canada, n.d.: 2)

Citizens cannot possibly comply with every risk avoidance tip issued by every institution, and they cannot 'safety-proof' every aspect of their daily routine. The futility of compliance says much about possible ulterior motives of institutions. Institutions recognize that nobody can comply with every safety protocol, and even if this were possible, the 70 percent of information leakages that are due to institutional practices would still exist. Responsibilization efforts are seemingly misleading, as responsibilization trajectories (i.e. the complete protection of personal information) are doomed to fail. In fact, institutions *expect* responsibilization to fail. Statements such as "[Y]ou probably can't prevent identity theft entirely" (PhoneBusters, n.d.-c) are common. What countless responsibilization measures do accomplish is to insulate institutions from blame once victimization has occurred. Even though compliance with every risk tip is impossible, institutions use instances of non-compliance to shift responsibility onto the victims, insinuating that they have triggered their own victimization.

Accordingly, when victimized, citizens are directed to look for flaws in their own behaviour. They unquestioningly bear a *de facto* reverse onus in establishing that

CANADIAN THESES
THÈSES CANADIENNES

WHITSON, Jennifer Robin
ASSUMED IDENTITIES: RESPONSES TO IDENTITY THEFT IN AN ERA ...

ISBN 978-0-494-22182-2
MR-22182

they have been victimized and then proving that they did everything in their power to avoid this victimization. Amidst the bureaucratic struggle to establish their innocence, victims have neither the time nor the support to look for flaws in institutional systems that have failed to protect them. Victims are encouraged to criticize themselves (e.g. blaming their 'stolen identity' on shopping online, giving out their personal information to a telephone solicitor, or not checking their credit report more often), rather than criticizing how government and corporate information regimes have precipitated the conditions for their victimization.

These ordeals and paperwork are ultimately geared to return the citizen to the status of a routine transaction in a technological system. When the knowledge network is working according to institutional desires, individual subjects are rendered anonymous—they are just another transaction, another PIN, another stream of unremarkable information that can be compiled into another unremarkable data double. In this system, subjectivity and the failure to be reduced to a transaction presents a problem; it is an inefficiency calling for more time, effort, and expense put into a relationship that should be impersonal, quickly logged, and then forgotten except for further profiling efforts. Identity theft challenges the stability of the system and awakens individuals (and institutions) to the notion that this informational regime is insecure and poses risks. The functioning of the entire network is put at risk by the concerns of those who are reticent to divulge information for fear of victimization. Therefore, identity theft discourses, responsibilization tips, and the ordeals victims must go through in order to re-establish their 'identity', are all geared to lessen the 'noise' in

the network by attempting to assuage client's concerns, and once more coax them to participate in the informational network.

The consequences of these efforts to coax participation in the network go beyond issues of just identity theft. Conversely, in the creation of a late modern hyper-vigilant subject, institutions are creating a subject whose scope of choices for action is highly circumscribed. By 'patterning' individuals so tightly into the information system, institutions remove the agency of victims and instead promote their objectification. The most apparent way this is achieved is through the institutional formatting of communication, removing the ability of victims to respond to identity theft in any way other than those pre-approved and contrived by institutions. To fully understand the matter, we must return to the issue of Automated Socio-Technical Environments (ATSEs).

Given the characteristics of ASTEs that were discussed in the first chapter—e.g. that data doubles supplant humans in institutional importance, and accordingly, ASTEs becoming targets of identity thieves—it is paradoxical that institutional responses to identity theft encourage further dependence on these self-same processes. A telling example of this dependence can be seen by examining institutionally endorsed methods for reporting identity theft. These methods rely heavily on ASTEs and for the most part preclude human interaction—instead relying on technological environments to format victimization reports in a way that is easily databased and analysed.

The four steps for identity theft victims to follow that were listed near the beginning of this chapter serve to exemplify just how much interaction and communication is formatted through the use of ASTEs. The first recommended step is

to contact the police and file a report. Although institutions cast doubt on law enforcement's ability to respond to identity theft—as demonstrated by the CBA warning victims that "[d]ue to the nature of the crime, police can determine very little from one incident"(Canadian Bankers Association, 2004b)—the report serves a secondary function. It becomes the "proof" of victimization victims need to convince institutions that they are not fraudulent offenders. "A police report is helpful both in demonstrating to would-be creditors and debt collectors that the consumers are victims of identity theft, and also serves as an 'identity theft report' that can be used for exercising various rights under the newly enacted Fair and Accurate Credit Transactions Act" (Federal Trade Commission, 2005b). Victims are referred not to physical police agencies, but to online reporting systems such as the RCMP's RECOL or the FBI's IC3, where the experiences of victims are converted into "fill in the blanks" and easily analysable but de-contextualized statistical data.

The second and third steps involve notifying the major Credit Bureaus and financial institutions, and again rely on filling in the blanks, this time in the ubiquitous form of Identity Theft Affidavits, which were discussed earlier in this chapter. The final step, contacting Government Authorities such as PhoneBusters and the FTC, is perhaps the most fully dependent on ASTEs—leaving victims few options but to go online and divulge the particulars of their victimization, including their personal identification and information. Contact information for alternative reporting methods such as telephone numbers or office addresses is rare. The oft repeated reporting mantra sounds like this: "If you or someone you know is a victim of identity theft, please visit www.consumer.gov/idtheft. The information you enter there becomes part of a secure

database that's used by law enforcement officials across the nation to help stop identity thieves" (Federal Trade Commission, 2003a). Victims likely feel a loss of agency, because the experience is a 'one-way mirror'. They often have no clear idea of who their reported information is intended for, where it goes, and what it is used for (Ericson & Haggerty, 1997). All that is known is that reported information enters unknown databanks, is supposedly disseminated for their own benefit, and is necessary for the reclamation of their 'identity'.

It is ASTE intermediaries like online reporting venues that act to bind actors into the system while simultaneously removing their freedom of choice. This is achieved by structuring individuals' behaviour in ways that promote the continued operation of the information network while constraining the ability to behave in alternative ways. Institutions force people to model their behaviour according to the dictates of the technological system.

In a social system based on access and denial, individuals are theoretically able to act in ways not dictated by institutions. In reality, in order to get cash from the ATM, to shop online at Amazon, or even to report identity theft victimization, citizens *must* behave in a certain way, to give information to certain institutions, and to follow their recommendations exactly or face the repercussions (e.g. denial of service, denial of claims for remuneration, etc.). Technology by and large works in linear ways that pattern subjects' actions accordingly, and any non-linear, non-pre-approved behavior results in failure to gain access to the system.

The fact that ASTEs are composed of information gleaned from data doubles also is a cause for concern. ASTEs, while providing mandated service, collect

information on users, compile it into data doubles, and transmit this information back to institutions. The information collected is used to improve the functioning of ASTEs, but it is also used in future decision making, (e.g. when determining how to improve service, where service should be cut, which type(s) of customers should be catered to, and conversely which type(s) should be avoided). ASTEs rely on tracking people's actions, and make no effort to understand or even record individual motivations and mentalities. As such, surveillance in the form of ASTEs creates an approximation of who a person really is. The "recorded data is but a snapshot in time, easily taken out of context, and devoid of the essential meanings with which humans accord their behaviours" (Ball & Webster, 2003: 14). Yet, in terms of government, law enforcement and corporate decision making, this objectified subject is a documentary identity that takes precedence in decision making.

The reliance on data doubles is troubling because, unlike real people, data doubles are non-responsive. Data doubles and ASTEs promote a panoptic sort, the constant screening of user profiles, looking to deny goods and services for those users who are unprofitable or incompliant, thereby promoting a system of exchange based on access and denial, and selective marketing based on increasingly precise user profiles. Routine decisions are accordingly made via surveillance and the thresholds established in the panoptic sort, rather than the desires and needs of real citizens. Data doubles, unable to respond to or critique governing institutions, become the objects of governance. The complex, rich subjects upon which data doubles are based are increasingly rendered impotent.

In summary, institutions organize and direct individuals in ways that strengthen and stabilize conceptions of identity theft as a threat, and in doing so strengthen the link these actors have with the network of information exchange. They articulate responsibilization projects for individuals that effectively limit their scope of action, and in doing so, encourage a late modern hyper-vigilant subject whose range of response both to crimes and institutions themselves is severely limited.

Chapter 4: Identity Theft, Agency, and Resistance

This thesis is not exclusively about identity theft. It is also an examination of information capitalism in postmodern society. It is a story about the dehumanization, the reduction, and the potential elimination of the active agent in particular institutional contexts. Identity theft, the discourses surrounding it, and the measures aimed at information protection are just one locus of this dehumanization. The danger posed to individuals and their agency does not originate in identity theft alone, but focusing on identity theft in particular is a useful starting point. This fourth and final chapter highlights the ties between identity theft, information capitalism, and the loss of agency. These ties are important to the social sciences because they show how social subjects' autonomy over their information is shrinking at the same time as their set of potential responses is being limited.

Discourse analysis helps reveal the influence institutions have on how people comprehend and make sense of identity theft. Institutional depictions such as those explored in this research affect what is said and done about identity theft, and have direct consequences for the direction and character of individuals' action and inaction, especially in relation to the network of information exchange. These discourses allow certain things to be said (e.g. statements endorsing responsibilization as a means of data protection), and impedes other things (e.g. statements disputing institutions' right to demand personal information). Arguably the most important thing learned from this discourse analysis is that discourses on identity theft are subsumed under larger discourses on information exchange in the current technological era.

ASTEs allow institutions to streamline their processes, providing convenient, quick, and efficient automated services that disperse with 'unnecessary' human interaction. Their optimal functioning is dependent upon knowledge about their users—consumer data profiles that are generated and gathered during the use of the ASTE in question or are assembled from other sources. This knowledge is a powerful tool, allowing institutions to assess customers' needs, to cater to, and even influence their desires. Institutions use this knowledge to strengthen their own position by increasing their efficiency and identifying risky or unprofitable clientele. But this knowledge is also a target for thieves, and can be used to infiltrate victim's financial accounts and personal information, granting access and anonymity to criminals willing to assume another's name, account code or social insurance number for personal gain.

The realization that increasing amounts of personal information equates to increasing opportunities for this information to be stolen and misused makes some citizens reticent to divulge information or use possibly insecure services. But this information is the lifeblood of institutions—not only does it guide and support their daily operations, it is also a source of revenue. To maintain faltering informational flows, institutions encourage individuals to protect their information while they paradoxically divulge it to various other institutions. This apparent contradiction is overcome by directing informational flows to ostensibly legitimate sources and away from illegitimate sources. In order to direct these flows, institutions walk a fine line between encouraging the fear necessary to motivate individuals to protect their information, and convincing individuals to trust the system of information exchange.

For all their purported concern about victims, their demonstrated concern is incidental, since institutional efforts to counteract identity theft are ultimately concerned with shoring up the network of trust in information capitalism. These efforts are often beneficial to institutions, downloading the responsibility for protecting information onto individuals, and displacing blame for victimization onto those who purportedly fail to responsibilize 'correctly'. The danger posed by identity theft is continually contested, leading to tension between assurances of safety and 'no-loss guarantees' and institutional claims that they are largely powerless to stop this rapidly growing crime. Institutionally promoted protection efforts increase the reliance on ASTEs and further support the reduction of individual actors into identification numbers and statistics. This reduction occurs because ASTEs are constructed to respond to a limited range of behaviours. Ultimately, victims seem to be victimized less by thieves and more by institutions and the bureaucratic processes necessary for re-establishing and removing the miasma of criminality from their identity.

Institutions appear to have determined that social interactions not choreographed into pre-approved formatted linear functions are problematic because they are time consuming, and inefficient. This remains true even for those institutions that respond to crime, even though the reliance upon choreographed functions and ASTEs enables criminals' easy access to institutional databases and others' 'identities'. In response to the identity theft threat, institutions articulate projects for individual consumers that encourage a hyper-vigilant subject who is constantly monitoring themselves and altering their behaviour in response to institutional dictates. Surveillant methods aimed at combating identity theft have the potential for 'function creep', whereby reported

information is adopted for a variety of originally unplanned purposes. A fundamental problem with surveillant technologies is they encourage the idea that progress can be achieved through techno-salvation, and therein the solutions to identity theft lie in even more surveillance. Convictions such as these fuel the growth of more surveillance, enabling it to become more intrusive and colonize more areas of life (Marx, 1995: 238). This is compounded by the inability to prove that surveillance as a method of crime fighting and control does not work, as failures to predict and limit crime encourage fear and emphasize the need for further surveillance.

Responding to deviance with technical security solutions creates a "dialectic wherein new solutions offer new challenges to violators which in turn create a need for new solutions by social controllers" (Marx, 1995: 241). The attempts to protect documentary identity while simultaneously increasing reliance on it in terms of government, economic, and even social interactions, are at best futile and at worst a motivating challenge for potential criminals. It therefore follows that "the most prolific area of criminal activity will be identity-related, because once offenders have broken into the system, then they will be free to help themselves" (Levi & Wall, 2004: 213).

Despite endless responsibilization tips, the hyper-vigilant subject is recognized as being powerless to prevent their victimization. The fear and anxiety surrounding identity theft spurs them to undertake complicated and sometimes contradictory protection procedures, yet it is impossible to follow every recommendation. Adhering to these recommendations is frequently a dead-end given that the majority of information leaks are due to institutional security breaches; and by the time the breach is discovered, the harm is done. Patterned into responding in predetermined ways, and

forced to accept guilt for any real or imagined behaviours that may have precipitated their victimization, individuals have no other choice but to continue following the dictates of the informational system. They are forced to format their behaviours in alignment with the requirements of ASTEs as other avenues for response are ineffective or ignored. They become button pushers and card numbers, more object than subject.

Institutions, by endorsing and basing the provision of services on ASTEs force consumers to participate in an insecure network of information exchange. ASTEs foster an exclusionary society in that those who refuse to comply (e.g. those who spurn credit cards, or refuse to disclose their social security number, or do not behave according to a predetermined schedule of actions), are excluded from the system, and are barred from receiving a variety of services such as health benefits, discounted prices, certain banking options, and insurance coverage. While human agency still exists, as people can still choose to participate or not and can either withhold information or disclose it, this presents a greater danger. Governing citizens through their desire for quick and efficient service and a wider range of products and services subtly compels their actions. Thinking 'rationally', people accept the system of information exchange because although there are alternatives, none of them are desirable. For example, it is drastically easier to follow institutional instructions and report identity theft via plugging in blanks on pre-approved forms, sending the forms off, and waiting for a resolution, even if they require excessive amounts of information. Dealing with every affected institution without mediating the conversation via structured forms and on-line reporting is incredibly time-consuming, if not impossible. It is also frustrating given that victimization reports that are not structured into pre-approved, easily analyzable forms,

generally cannot be 'processed', and the longer one takes to process their report, the more liable they are for losses.

There seems to be few avenues of resistance to these trends. Theoretically, "discourses 'channel' rather than 'control' the discursive possibilities, facilitating some things being said and other things being impeded" (Purvis & Hunt, 1993: 486). Institutional discourses should not be able to blithely generate subject positions into which people are 'inserted' without any potential for struggle, resistance, or negotiation, yet, this is exactly what seems to be taking place. Individuals are markedly compliant in acceding to institutional requests for information. The discourses detailed in the previous chapters help to formulate and cement individual's beliefs about the advantages of, and the need for, providing such information. Institutions rely on the trust that individuals have in 'official' authority to override any reticence to divulge information. Lack of resistance to data gathering ventures may also be masked as acceptance because of a fear of losing one's access privileges or as a necessary condition for something desired such as employment, credit, government benefits, and even remuneration for losses due to identity theft (Marx, 2003). Marx, in detailing resistance to surveillance, lists techniques of neutralization, and asserts that "[p]eople will break rules if they regard an organization or its surveillance procedures as unacceptable or illegitimate, untrustworthy, or invalid, demeaning, unnecessary, or irrelevant" (2003: 373). But in this case, the fear of identity theft itself, and the fear of institutional reprisals for not divulging information, helps to ensure the compliance of individuals.

Resistance against surveillance exists, but this resistance is largely directed towards 'illegitimate' surveillants such as 'identity thieves'. Monitoring one's credit report and financial statements helps to pinpoint account tampering and react quickly to illegitimate surveillance, but these 'discovery moves' increase institutional surveillance (Marx, 2003). For example, although credit reports may help detect identity thieves, they also authorize credit reporting companies to increase their surveillance.

Other forms of resistance only work in a limited form. Some surveillance can be passively avoided by withdrawing from the system of information exchange, but this withdrawal only succeeds in a limited context (Marx, 2003). For example, citizens can avoid customer loyalty cards which track their shopping habits, but they cannot avoid divulging requested information on tax filings or police reports. In terms of avoiding the increased surveillance and hassle that occurs once one has been a victim of identity theft, the best recourse is to avoid reporting identity theft altogether and in doing so, renounce any claims to remuneration.

Counter-technologies to surveillance in the sphere of identity theft are limited. Citizens can counter identity thieves by accepting the increased surveillance of institutions, but they generally cannot counter the surveillance of institutions themselves. Due to the nature of information capitalism, *all* institutions depend on increased data about their clientele, and as such, switching to another institution that does not surveil is not viable. The only option is switching to institutions that promise a lesser extent of surveillance, or alternatively promise to protect the information that they accumulate. As a note of interest, there is one method to avoid institutional surveillance: it is to mask one's personal information by falsifying one's identifiers or

assuming another's. Therefore, an ironic solution to the increased institutional surveillance precipitated by identity theft is to become an identity thief oneself.

Eschewing the above noted method to avoid victimization, individuals are so focused on shredding up receipts and upgrading internet security that they avoid looking at the criminogenic conditions that institutions generate. They fail to recognize that institutions themselves have created these conditions and are doing little to improve them. Proposed institutional security and responsibilization measures are a stop-gap. Even when individuals recognize that institutions are largely at fault for this 'new' crime and the anxiety and suspicion it precipitates, they are rendered virtually powerless to do anything about it. This powerlessness can be exemplified best by imagining how I, an academic who is more informed than most on the subject of identity theft, would respond to the hypothetical possibility (and perhaps the future reality) of having my identity 'stolen'.

Personally, I recognize that American Express gathers information on where I shop, what I buy, and how much I spend, and uses this information to target me with unwanted mail and promotional items. But what choice do I have, other than the rare opportunity to read the fine print and opt out? All credit card companies do this, and I require a credit card to purchase goods and services, such as the latest on-line computer security downloads or to book a hotel room for my next conference. Should the inevitable happen, and I discover that someone has been making purchases on my credit card; I will have to go through the ordeal of disputing the fraudulent charges. I recognize that the forms and affidavits that I will be instructed to fill out will be used to scour my actions and deflect suspicion and responsibility for my victimization back

upon myself, yet, these forms are necessary to report the crime, and reporting the crime is a precondition to being reimbursed for money stolen from me and re-establishing my credit rating and 'identity'. I am powerless to prevent my own victimization: both at the hands of the criminals and perhaps more distressingly, at the hands of the very institutions I am forced to rely upon. Their practices have created the threat (e.g. valuing convenience over total security), their exhortations and warnings have created my anxiety (e.g. claiming that my credit rating may be irrevocably damaged), their endless security precautions have cost me time and money (e.g. buying a shredder and shredding all my receipts will not prevent this theft, and expensive identity theft protection will force me to deal with an unfathomable labyrinthine teleservice), and in the end, my 'identity'—my credit card number, my bank account, and even my credit report—will still be put at risk. This is likely not because of anything I have done or failed to do—most information leaks reside at the institutional level (in this case it could be an unscrupulous Amex employee, or an insecure online site that purports to be safe, or hotel computers that are thrown out without first erasing all the customer data on them). Irrespective, my victimization will continue. I will still need to fill out every blank on every monotonous form. I will still need to contact every credit reporting agency and every financial institution I deal with alongside numerous law enforcement and consumer protection agencies. I will be forced to report on myself, knowing that the information that I will be pressured to divulge will be used to surveil me even further, to compress me into a statistic, a data profile, an occurrence, and in doing so create another opportunity for the this information to be misused and harm me again, but I am powerless. I will grudgingly become the late modern subject. I will become

hyper-vigilant, always suspicious and ridden by anxiety. Even armed with knowledge, I will be incapable of responding to an occurrence of identity theft in any way other than that dictated by the institutions who guide the information network. Accordingly, this thesis goes beyond just identity theft and is important for the whole of social sciences because the prospect of identity theft patterns people's behaviour and limits their responses, changing the way in which subjects relate to institutions.

Bibliography

Alberta Government Services. (2004). Consumer tips: Identity theft. Retrieved 2005/05/17, 2005, from http://www3.gov.ab.ca/gs/pdf/tipsheets/Identity%20theft.pdf

American Express. (2003). Preventing identity theft: Steps to prevent id theft. Retrieved June 21, 2005, from http://home3.americanexpress.com/corp/cr/fraud/protect_identity.asp

American Express. (2004a). American Express adds free identity theft assistance to its line-up of cardmember benefits. Retrieved December 12, 2005, from http://home3.americanexpress.com/corp/pc/2004/id_theft.asp

American Express. (2004b). Fraud prevention: Data security requirements FAQs. Retrieved 2005/06/22, 2005, from http://www125.americanexpress.com/merchant/oam/ns/USEng/FrontServlet?request_type=navigate&page=dataSecurityFAQ

American Express. (2004c). Fraud prevention: General requirements. Retrieved 2005/06/22, 2005, from http://www125.americanexpress.com/merchant/oam/ns/USEng/FrontServlet?request_type=navigate&page=generalRequirements

American Express. (2004d). Internet privacy statement: What information we collect and how we use it. Retrieved June 22, 2005, from www10.americanexpress.com/sif/cda/page/0,1641,17215,00.asp

American Express. (2005a). Fraud protection center: What you can do to prevent fraud. Retrieved June 21, 2005, from https://www124.americanexpress.com/cards/loyalty.do?page=FraudCenter.whatyoudo

American Express. (2005b). Identity theft assistance: Information for recovering your good name. Retrieved May 20, 2005, from https://www124.americanexpress.com/cards/FraudCenter/common/pdf/VictimPackage.pdf

American Express. (2005c). Identity theft assistance: Safeguarding your identity. Retrieved May 17, 2005, from https://www124.americanexpress.com/cards/FraudCenter/common/pdf/InterestPackage.pdf

American Express. (n.d.-a). Fraud protection center: Tools and resources. Retrieved June 21, 2005, from https://www124.americanexpress.com/cards/loyalty.do?page=FraudCenter.toolsandresources

American Express. (n.d.-b). Fraud protection guarantee. Retrieved June 21, 2005, from https://www124.americanexpress.com/cards/loyalty.do?page=fraudprotection.guarantee

American Express. (n.d.-a). Fraud prevention: Fraud FAQs. Retrieved 2005/06/22, 2005, from http://www125.americanexpress.com/merchant/oam/ns/USEng/FrontServlet?request_type=navigate&page=fraudPreventionFAQ

American Express. (n.d.-b). Fraud protection center: CreditSecure. Retrieved June 21, 2005, from https://www124.americanexpress.com/cards/loyalty.do?page=FraudCenter.creditsecure

American Express. (n.d.-c). Fraud protection center: CreditSecure frequently asked questions. Retrieved June 21, 2005, from https://www124.americanexpress.com/cards/loyalty.do?page=FraudCenter.creditsecurefaq

American Express. (n.d.-d). Fraud protection center: Tools and resources. Retrieved June 21, 2005, from https://www124.americanexpress.com/cards/loyalty.do?page=FraudCenter.toolsandresources

American Express. (n.d.-e). Fraud protection guarantee. Retrieved June 21, 2005, from https://www124.americanexpress.com/cards/loyalty.do?page=fraudprotection.guarantee

American Express. (n.d.-f). Fraud protection center: What is fraud. Retrieved 2005/06/21, 2005, from https://www124.americanexpress.com/cards/loyalty.do?page=FraudCenter.whatisfraud

American Express. (n.d.-g). Identity theft assistance: Safeguarding your identity. Retrieved May 17, 2005

American Express. (n.d.-h). Learn more about alerts. Retrieved 2005/06/21, 2005, from https://www65.americanexpress.com/alerts/un/LearnMore.jsp

Ball, K., & Webster, F. (2003). The intensification of surveillance. In K. Ball & F. Webster (Eds.), *The intensification of surveillance: Crime, terrorism and warfare in the information age* (pp. 1-15). London; Sterling, VA: Pluto Press.

Bauman, Z. (2002). Violence in the age of uncertainty. In A. Crawford (Ed.), *Crime and insecurity: The governance of safety in Europe* (pp. 52 - 73). Devon: Willan.

Beck, U. (1992). Modern society as a risk society. In N. Stehr & R. V. Ericson (Eds.), *The culture and power of knowledge: Inquiries into contemporary societies* (pp. 199 - 214). Berlin; New York: W. de Gruyter.

Best, J. (2001). *Damned lies and statistics: Untangling numbers from the media, politicians, and activists*. Berkeley: University of California Press.

Bi-national Working Group on Cross-Border Mass Marketing Fraud. (2004). Identity theft: A report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States. Retrieved May 17, 2005, from http://www.psepc.gc.ca/publications/policing/identity_theft_e.asp

Canadian Bankers Association. (2003a). Fraud and security: Efforts with others. Retrieved May 17, 2005, from http://www.cba.ca/en/print.asp?fl=4&s1=268&t1=289&docid=493&pg=1

Canadian Bankers Association. (2003b). Identity theft: A policy is needed. Retrieved May 17, 2005, from www.cba.ca

Canadian Bankers Association. (2004a). The banking industry in Canada: Taking a closer look. Retrieved May 17, 2005, from http://www.cba.ca/en/content/publications/2005CBAAnnRepFINAL.pdf

Canadian Bankers Association. (2004b). Safeguarding your money: A guide to protecting your money and resolving bank problems. Retrieved May 20, 2005, from http://www.cba.ca/en/content/publications/EngSafeguardingFinal.pdf

Canadian Bankers Association. (2005a). Fraud and security: E-mail fraud. Retrieved May 17, 2005, from http://www.cba.ca/en/print.asp?fl=3&sl=308&tl=312&docid=570

Canadian Bankers Association. (2005b). Fraud and security: Identity theft. Retrieved May 17, 2005, from http://www.cba.ca/en/viewdocument.asp?fl=3&sl=65&tl=136&docid=478&pg=1

Canadian Bankers Association. (2005c). Protecting your personal information online. Retrieved May 17, 2005, from http://www.cba.ca/en/print.asp?fl=3&sl=308&tl=314&docid=499&pg=1

Castells, M. (2000). *The rise of the network society* (2nd ed.). Oxford; Malden, MA: Blackwell Publishers.

Castells, M. (2001). *The internet galaxy: Reflections on the internet, business, and society*. Oxford; New York: Oxford University Press.

Chan, J. (2001). The technological game: How information technology is transforming police practice. *Criminal Justice, 1*(2), 139 - 159.

CNN. (2005). ChoicePoint: More id theft warnings. Retrieved October 25, 2005, from http://money.cnn.com/2005/02/17/technology/personaltech/choicepoint/

Consumer Measures Committee. (2004). The identity theft statement: Frequently asked questions. Retrieved May 20, 2005, from http://cmcweb.ca/epic/internet/incmc-cmc.nsf/en/fe00077e.html

Consumer Measures Committee. (2005). Working together to prevent identity theft: A discussion paper. from http://www.gov.ab.ca/home/public_consultations/consultationpaper.pdf

Crawford, A. (2002). Introduction: Governance and insecurity. In A. Crawford & University of Leeds. (Eds.), *Crime and insecurity: The governance of safety in Europe*. Devon: Willan.

Deleuze, G. (1992). Postscript on societies of control. *October, 59*(Winter), 3 - 7.

Deleuze, G. (1997). Postscript on societies of control. In N. Leach (Ed.), *Rethinking architecture: A reader in cultural theory*. London: Routledge.

Elmer, G. (2003). A diagram of panoptic surveillance. *New Media & Society, 5*(2), 231 - 247.

Ericson, R. V., & Haggerty, K. D. (1997). *Policing the risk society*. Toronto: University of Toronto Press.

Federal-Provincial-Territorial Consumer Measures Committee. (2005). Identity theft: Protect your business, protect your customers. Retrieved May 17, 2005, from http://cmcweb.ca/epic/internet/incmc-cmc.nsf/vwapj/busidtheftkit.pdf/$FILE/busidtheftkit.pdf

Federal Bureau of Investigation. (2004a). A conundrum: How do you prevent crimes that haven't been born yet? Retrieved May 20, 2005, from http://www.fbi.gov/page2/cyberterrorism022504.htm

Federal Bureau of Investigation. (2004b). Don't let this happen to you! How to protect your good name from identity theft. Retrieved May 20, 2005, from http://www.fbi.gov/page2/oct04/preventidt102104.htm

Federal Bureau of Investigation. (2004c). Protecting yourself against identity theft? Sometimes that's not enough. Retrieved May 20, 2005, from http://www.fbi.gov/page2/sept04/idtheft090304.htm

Federal Bureau of Investigation. (n.d.-a). Common fraud schemes. Retrieved 05/20, 2005, from https://www.fbi.gov.majcases/fraud/fraudschemes.htm

Federal Bureau of Investigation. (n.d.-b). Internet fraud. Retrieved May 20, 2005, from https://www.fbi.gov/majcases/fraud/internetschemes.htm

Federal Trade Commission. (2003a). Id theft: What's it all about? Retrieved 2005/05/17, 2005, from http://www.ftc.gov/bcp/conline/pubs/credit/idtheftmini.htm

Federal Trade Commission. (2003b). Privacy: What you do know can protect you. Retrieved May 20, 2005, from http://www.ftc.gov/bcp/conline/pubs/alerts/privprotalrt.htm

Federal Trade Commission. (2004a). Information compromise and the risk of identity theft: Guidance for your business. Retrieved 2005/05/20, 2005, from http://www.ftc.gov/bcp/conline/pubs/buspubs/idtrespond.htm

Federal Trade Commission. (2004b). Prepared statement of the Federal Trade Commission on identity theft and social security numbers before the Subcommittee on Social Security of the House Committee on Ways and Means. Retrieved May 20, 2005, from http://www.ftc.gov/os/testimony/040615idtheftssntest.pdf

Federal Trade Commission. (2005a). FTC consumer alert: What to do if your personal information has been compromised. Retrieved May 20, 2005, from www.ftc.gov/bcp/conline/pubs/alerts/infocompalrt.pdf

Federal Trade Commission. (2005b). FTC testifies on security of consumers' financial data. Retrieved 2005/05/20, 2005, from https://www.ftc.gov/opa/2005/04/financialdatatest.htm

Federal Trade Commission. (2005c). Identity theft focus of national consumer protection week 2005. Retrieved May 20, 2005, from http://www.ftc.gov/opa/2005/02/ncpw05.htm

Federal Trade Commission. (2005d). National and state trends in fraud & identity theft: January - December 2004. Retrieved June 21, 2005, from www.consumer.gov/idtheft/pdf/clearinghouse_2004.pdf

Federal Trade Commission. (2005e). Protecting consumers' data: Policy issues raised by ChoicePoint (pp. 1 - 21).

Federal Trade Commission. (2005f). Securing electronic personal data: Striking a balance between privacy and commercial and governmental use. Retrieved May 20, 2005, from http://www.consumer.gov/idtheft/pdf/ftc_04.13.05.pdf

Federal Trade Commission. (2005g). Take charge: Fighting back against identity theft (pp. 1 - 48). Retrieved June, 2005 from www.ftc.gov/bcp/conline/pubs/credit/idtheft.pdf

Federal Trade Commission. (n.d.-a). Filing a complaint with the FTC. Retrieved June 21, 2005, from http://www.consumer/gov/idtheft/filing_complaintwftc.html

Federal Trade Commission. (n.d.-b). Instructions for completing the id theft affidavit. Retrieved May 20, 2005, from www.consumer.gov/idtheft/pdf/affidavit.pdf

Federal Trade Commission. (n.d.-c). Remedying the effects of identity theft. Retrieved May 20, 2005, from http://www.ftc.gov/bcp/conline/pubs/credit/idtsummary.pdf

Finch, E. (2002). What a tangled web we weave: Identity theft and the internet. In Y. Jewkes (Ed.), *Dot.Cons: Crime, deviance and identity on the internet* (pp. 86-104). Cullompton: Willan.

Foucault, M. (1977). *Discipline and punish: The birth of the prison* (1st American ed.). New York: Pantheon Books.

Gandy, O. (1993). *The panoptic sort: A political economy of personal information.* Boulder, Colo.: Westview.

Gandy, O. (2003). Data mining and surveillance in the post-9/11 environment. In K. Ball & F. Webster (Eds.), *The intensification of surveillance: Crime, terrorism and warfare in the information age* (pp. 26 - 41). London; Sterling, VA: Pluto Press.

Garland, D. (2001). *The culture of control*. Chicago: University of Chicago Press.

Giddens, A. (1990). *The consequences of modernity*. Stanford, Calif.: Stanford University Press.

Haggerty, K. D. (2001). *Making crime count*. Toronto: University of Toronto Press.

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *British Journal of Sociology, 51* (4), 605-622.

Industry Canada. (2004a). Privacytown overview. Retrieved May 20, 2005, from http://strategis.ic.gc.ca/epic/internet/inoca-bc.nsf/en/ca01360e.html

Industry Canada. (2004b). Privacytown voluntary privacy codes. Retrieved May 20, 2005, from http://strategis.ic.gc.ca/epic/internet/inoca-bc.nsf/en/ca01360e.html

Jewkes, Y. (2002). Policing the net: Crime, regulation and surveillance in cyberspace. In Y. Jewkes (Ed.), *Dot.Cons: Crime, deviance and identity on the internet* (pp. 15 - 35). Cullompton: Willan.

Jones, R. (2000). Digital rule: Punishment, control and technology, *Punishment & Society* (Vol. 2, pp. 5 - 22): Sage Publications, Ltd.

Latour, B. (2004). Gabriel Tarde and the end of the social. *Distinktion: Scandinavian Journal of Social Theory, 9*, 33 - 47.

Latour, B. (2005). *Reassembling the social: An introduction to actor-network-theory.* Oxford; New York: Oxford University Press.

Law, J. (1992). Notes on the theory of the actor network: Ordering, strategy and heterogeneity. Retrieved January 27, 2006 from http://www.lancs.ac.uk/fss/sociology/papers/law-notes-on-ant.pdf

Law, J., & Hassard, J. (1999). *Actor network theory and after*. Oxford; Malden, MA: Blackwell.

Levi, M. (2001). "Between the risk and the reality falls the shadow": Evidence and urban legends in computer fraud (with apologies to T.S. Eliot). In D. Wall (Ed.), *Crime and the internet* (pp. 44 - 58). London; New York: Routledge.

Levi, M., & Wall, D. S. (2004). Technologies, security, and privacy in the post-9/11 European information society, *Journal of Law & Society* (Vol. 31, pp. 194 - 206): Blackwell Publishing Limited.

Lianos, M., & Douglas, M. (2000). Dangerization and the end of deviance. *British Journal of Criminology, 40*, 261 - 278.

Lourdeau, K. (2004). Testimony of Keith Lourdeau, Deputy Assistant Director, Cyber Division, FBI. Before the Senate Judiciary Subcommittee on Terrorism, Technology and Homeland Security. Retrieved May 20, 2005, 2005, from http://www.fbi.gov/congress/congress04/lourdeau022404.htm

Lyon, D. (2001). Under my skin: From identification papers to body surveillance. In J. Caplan & J. C. Torpey (Eds.), *Documenting individual identity: The development of state practices in the modern world* (pp. 291 - 310). Princeton, N.J.: Princeton University Press.

Marx, G. T. (1995). The engineering of social control: The search for the silver bullet. In J. Hagan & R. D. Peterson (Eds.), *Crime and inequality* (pp. 225 - 246). Stanford, Calif.: Stanford University Press.

Marx, G. T. (2003). A tack in the shoe: Neutralizing and resisting the new surveillance. *Journal of Social Issues, 59*(2), 369 - 390.

National White Collar Crime Center, & Federal Bureau of Investigation. (2005). IC3 2004 internet fraud crime report: January 1, 2004 - December 31, 2004. Retrieved June 21, 2005 from www.ifccfbi.gov/strategy/2004_IC3Report.pdf

Nock, S. L. (1993). *The costs of privacy: Surveillance and reputation in America*. New York: Aldine De Gruyter.

O'Hara, K. (2004). *Trust: From Socrates to spin*. Cambridge: Icon Books Ltd.

O'Harrow, R. J. (2005, February 17). Id data conned from firm: ChoicePoint case points to huge fraud. Retrieved November 24, 2005, from http://www.washingtonpost.com/wp-dyn/articles/A30897-2005Feb16.html

O'Neill, O. (2002). *A question of trust*. Cambridge: Cambridge University Press.

Office of the Privacy Commissioner of Canada. (2003, July 25, 2004). Protecting your privacy on the internet. Retrieved May 17, 2005, from http://www.privcom.gc.ca/fs-fi/02_05_d_13_e.asp

PhoneBusters. (n.d.-a). About us. Retrieved August 3, 2005, from http://www.phonebusters.com/english/aboutus.html

PhoneBusters. (n.d.-b). Identity theft complaints: 2003. Retrieved May 20, 2005, from http://www.phonebusters.com/english/statistics_E03.html

PhoneBusters. (n.d.-c). Identity theft: Could it happen to you? Retrieved May 20, 2005, from http://www.phonebusters.com/english/recognizeit_identitythe.html

PhoneBusters. (n.d.-a). Identity theft: Could it happen to you? Retrieved May 20, 2005, from http://www.phonebusters.com/english/recognizeit_identitythe.html

PhoneBusters. (n.d.-b). Identity theft: Tips that will help you minimize your risk. Retrieved December 21, 2005, from http://www.phonebusters.com/english/recognizeit_identitythetips.html

Purvis, T., & Hunt, A. (1993). Discourse, ideology, discourse, ideology, discourse, ideology. *The British Journal of Sociology, 44*(3), 473 - 499.

Reporting Economic Crime Online. (n.d.). Identity fraud. Retrieved 2005/05/20, 2005, from https://www.recol.ca/scams/Identity_Fraud.aspx

Royal Canadian Mounted Police. (2003, December 22). Identity theft. Retrieved May 17, 2005, from http://www.rcmp-grc.gc.ca/scams/identity_e.htm

Royal Canadian Mounted Police. (2004). Counterfeiting and credit card fraud. Retrieved May 17, 2005, from http://www.rcmp-grc.gc.ca/scams/ccandpc_e.htm

SafeCanada. (2005). Identity theft - questions and answers. Retrieved May 17, 2005, from http://www.safecanada.ca/identitytheft_e.asp

Simon, J. (2000). Megan's law: Crime and democracy in late modern america. *Law & Social Inquiry, 25*(4), 1111 - 1150.

Solicitor General Canada. (n.d.). Public advisory: Special report for consumers on identity theft. D. o. Justice (pp 1 - 5).

Wall, D. (2001). Maintaining order and law on the internet. In D. Wall (Ed.), *Crime and the internet* (pp. 167 - 183). London; New York: Routledge.

Wall, D. (2002). Insecurity and the policing of cyberspace. In A. Crawford (Ed.), *Crime and insecurity: The governance of safety in Europe* (pp. 186 -209). Devon: Willan.

Wall, D. (2006). Surveillant internet technologies and the growth in information capitalism: Spams and public trust in the information society. In K. Haggerty & R. Ericson (Eds.), *New politics of surveillance and visibility*. Toronto: University of Toronto Press.

Weber, H. R. (2005, July 11). Chief ChoicePoint screener says no employees involved in breach. Retrieved November 24, 2005, from http://www.signonsandiego.com/news/business/20050711-1403-choicepoint.html

Williams, J. W. (2005). Reflections on the private versus public policing of economic crime. *British Journal of Criminology, 45*, 316 - 339.